BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 31-401

1 JANUARY 1999

AIR FORCE MATERIEL COMMAND
Supplement 1

3 DECEMBER 1999

Security

INFORMATION SECURITY PROGRAM MANAGEMENT

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the SAF/AAD WWW site at: http://afpubs.hq.af.mil. If you lack access, contact the Air Force Publishing Distribution Center (AFPDC).

OPR: HQ USAF/XOFI (Deborah Ross)
HQ AFMC/SF (Peter C. Bryant)

Certified by: HQ USAF/XOF
(Brig Gen Richard A. Coleman)
HQ AFMC/SF (Francis L. Cooper)

Supersedes AFI 31-401, 22 Jul 94 and AFI 31-401/AFMC Sup 1, 20 November 1996.

Pages: 76
Distribution: F

It contains Air Force (AF) unique guidance needed to supplement Air Force Policy Directive (AFPD) 31-4, *Information Security*; Executive Order (EO) 12958, *Classified National Security Information*, 20 Apr 95; Office of Management and Budget (OMB), Information Security Oversight Office (ISOO) Directive Number 1, *Classified National Security Information,* 13 Oct 95; and, Department of Defense (DoD) 5200.1-R, *Information Security Program*, 17 Jan 97, for the management of the Air Force Information Security Program. Additional references include DoD Instruction (DoDI) 5240.11, *Damage Assessments*, 23 Dec 91; and, DoD Directive (DoDD) 5210.83, *Unclassified Controlled Nuclear Information (UCNI)*, 15 Nov 91. All these references together describe how to protect and handle classified information. For user convenience, specific policy references are listed at the end of each paragraph where applicable.

(AFMC) This supplement applies to the US Air Force Reserve units and members.

SUMMARY OF REVISIONS

This document is substantially revised and must be completely reviewed.

This publication of Air Force Instruction (AFI) 31-401 aligns guidance with the crrent Air Force and DoD policy established by EO 12958, and the Federal Register Part VI, Office of Management and Budget, 32 CFR Part 2001, Information Security Oversight Office; *Classified National Security Information; Final Rule,* 13 Oct 96. Most of the paragraphs within this AFI have been revised so specific changes are not highlighted. Revisions include renumbering the chapters so they conform with DoD 5200.1-R; adding prescribed forms; updating office symbols and publication references; identifying specific DoD policy for

each policy topic; requiring supervisors to rate employees on their handling of classified information; providing policy on Restricted Data; encouraging command level Information Security Program Managers (ISPM) to visit base level units; requiring base level ISPMs to do program reviews; requiring offices of primary responsibility to send security classification guides (SCG) to the Air Force Declassification Office (AFDO); describing declassification officials scope of authority; implementing automatic declassification of historical information 25 years old and older; implementing marking requirements under Executive Order (EO) 12958; identifying the Special Security Office (SSO) as the office responsible for implementing intelligence policy; expanding the safeguarding portion to address access requirements; adding more extensive guidance on accounting for and controlling classified information; expanding guidance on classified meetings and conferences; clarifying guidance for protecting classified material on aircraft located in foreign countries; providing guidance for all machines used for copying classified material; giving military commanders authority to determine appropriate security measures if standard requirements cannot be met; clarifying when to record destruction; authorizing ISPMs to approve alternative or compensatory security controls; requiring ISPMs to notify HQ USAF/XOFI when alternative or compensatory controls are approved; requiring personnel to ask owners of other agency information for permission to release the information outside the Department of Defense (DoD); adding guidance on the use of General Services Administration (GSA) contract carriers to courier classified material; providing safeguarding guidance for First Class Mail with the Postmaster notice; requiring activities to report delinquent receipts as security incidents; reducing the authority level for approving handcarrying classified material; clarifying documentation required for handcarrying classified material; clarifying training requirements; requiring budgeting for training needs; deleting preliminary inquiries; adding policy for classifying notices of security incidents; clarifying the investigative requirements and process; requiring copies of all damage assessment reports be sent to HQ USAF/XOFI; adding a list of references; updating the glossary of acronyms; updating the list of Critical Nuclear Weapon Design Information (CNWDI) officials; incorporating the Air Force Automatic Declassification Plan; and, obsoleting AF Form 608, Nickname Assignment/Change/Cancellation Request.

(AFMC) This supplement has been extensively revised and will require thorough review.

AFI 31-401, 1 January 1999, is supplemented as follows:

Chapter 1

POLICY AND PROGRAM MANAGEMENT

1.1. Policy. It is Air Force policy to identify, classify, downgrade, declassify, mark, protect, and destroy its classified information and material consistent with national policy. This general policy statement also applies to unclassified controlled information under the purview of relevant statutes, regulations and directives. *[Reference DoD 5200.1-R, Chapter 1, Section 1]*

1.2. Philosophy. Protecting information is critical to mission accomplishment. The goal of the Information Security Program is to efficiently and effectively protect Air Force information by delegating authority to the lowest levels possible; encouraging and advocating use of risk management principles; focusing on identifying and protecting only that information that requires protection; integrating security procedures into our business processes so that they become transparent; and, ensuring everyone understands their security roles and responsibilities and *takes them seriously*.

1.2. (AFMC) Installation and Headquarters Information Security Program Managers (ISPMs) implement and oversee the Information Security Program for the purpose of protecting collateral classified information. Other program infrastructures, independent of the ISPM, are established for protecting classified information in Special Access Program (SAP) and Sensitive Compartmented Information (SCI) arenas. The ISPM provides support to these areas when requested by appropriate authority within those channels. The ISP is an installation-wide program that provides services to all organizations, both permanent and tenant. To ensure a comprehensive and effective program, AFI 31-401 prescribes one ISPM per base and this title and authority is assigned to the Chief of Security Forces (CSF). There are some current exceptions to this policy in AFMC wherein the Director/Chief of Acquisition Security/Program Protection is assigned the ISPM role because of the large number of acquisition programs formerly assigned to product centers. The diminishing number of these programs now makes assignment of the ISPM function under the CSF the desired structure.

1.3. Program Management. The strength of the Air Force Information Security Program is in its infrastructure. The infrastructure is important because it facilitates effective communication of our security policies and procedures to those performing the Air Force mission. With the support of commanders at all levels, this is accomplished predominantly through our Information Security Program Manager (ISPM) and security manager system. Both play an integral role in ensuring unit personnel know and understand their role in protecting classified information against unauthorized disclosure. *[Reference DoD 5200.1-R, Chapter 1, Section 2]*

1.3.1. Senior Security Official. The Administrative Assistant to the Secretary of the Air Force (SAF/AA) is designated the Air Force Senior Security Official responsible for ensuring implementation of the Information Security Program.

1.3.2. Air Force Program Manager. The Chief, Information Security Division (HQ USAF/XOFI) is responsible for policy, resource advocacy, and oversight of this program.

1.3.3. Commanders of Major Commands (MAJCOM), Direct Reporting Units (DRU), Field Operating Agencies (FOA), and Installations. These commanders are responsible for:

1.3.3.1. Establishing information security programs.

1.3.3.2. Identifying requirements.

1.3.3.3. Executing their programs to comply with this policy.

1.3.4. Information Security Program Managers (ISPM). The Chief of Security Forces, senior security forces official or Director/Chief of Acquisition Security is designated the ISPM at every level of command, as appropriate. ISPMs:

1.3.4. (AFMC) The ISPM is responsible for providing standard services, as defined in information security program directives, to all organizations on the base. Organizations who can demonstrate that it is impractical to receive local ISPM support must submit a request for waiver to permit duplication of this support function IAW AFI 25-201, *Support Agreement Procedures*.

1.3.4.1. Manage Information Security Program implementation.

1.3.4.2. Provide oversight within their jurisdiction.

1.3.4.3. Provide and monitor training as required by **Chapter 8** of this AFI.

1.3.4.4. (Added-AFMC) ISPMs below MAJCOM level supplement this directive and provide an electronic copy to HQ AFMC/SFXP.

1.3.5. Unit Commanders or Equivalents. These commanders or equivalents will:

1.3.5.1. Appoint security managers to implement and manage the Information Security Program within the unit or staff agency.

1.3.5.1. (AFMC) Security manager duties in Air Force organizations are performed by military or DoD civilian employees. The role of security manager is generally assigned as an additional duty, but organizations who generate, process or store large amounts of classified may require a fulltime GS-080 Security Specialist to perform these duties.

1.3.5.2. Ensure security managers receive required training.

1.3.5.3. Execute their programs to comply with this policy.

1.3.6. Security Managers.

1.3.6.1. Set up the Information Security Program within their unit or staff agency.

1.3.6.2. Develop and update a unit security operating instruction.

1.3.6.2. (AFMC) The servicing ISPM provides assistance to security managers as required in the development of their security operating instructions.

1.3.6.3. Advise the unit commander or staff agency chief on security issues pertaining to the unit or staff agency.

1.3.6.4. Attend ISPM hosted security manager meetings.

1.3.6.5. Update and remind personnel of security policies and procedures.

1.3.6.6. Oversee the unit or staff agency self-inspection program.

1.3.6.7. Report security incidents immediately to the ISPM through their unit commander or staff agency chief.

1.3.6.8. Assist the unit commander or staff agency chief and ISPM in monitoring security incident investigations.

1.3.7. Supervisors:

1.3.7.1. Establish criteria, evaluate, and rate Air Force employees on their performance of security responsibilities. *[Reference DoD 5200.1-R, Paragraph 1-202g]*

1.3.7.1.1. Officer. See AFI 36-2402, *Officer Evaluation System,* paragraph 1.2.7.

1.3.7.1.2. Enlisted. See AFI 36-2403, *The Enlisted Evaluation System (EES),* paragraphs 1.1.9.2.

1.3.7.1.3. Civilian. See AFI 36-1001, *Managing the Civilian Performance Program,* paragraph 1.4.

1.3.7.2. Provide and ensure training as directed in **Chapter 8** of this AFI.

1.3.8. Sensitive Compartmented Information (SCI). The Director of Intelligence Surveillance and Reconnaissance (HQ USAF/XOI) is responsible for SCI policy.

1.3.9. Foreign Disclosure. The Deputy Under Secretary of the Air Force, International Affairs, (SAF/IA), 1080 Air Force Pentagon, Washington DC 20330-1080, oversees the release of Air Force classified information to foreign governments, persons, and international organizations.

1.3.10. Historian. The Air Force Historian (HQ USAF/HO), 500 Duncan Avenue, Box 94, Bolling AFB DC 20332-1111, approves or disapproves historical researchers access to classified information. *[Reference DoD 5200.1-R, Paragraph 6-201d]*

1.4. Oversight. In addition to using metrics for evaluating the effectiveness of the Information Security Program (see paragraph **1.7.**), these oversight practices will be implemented *[Reference DoD 5200.1-R, Chapter 1, Section 7]*:

1.4.1. MAJCOM, DRU, and FOA ISPMs will incorporate information security issues into Inspector General (IG) inspections/reviews. In addition MAJCOM, DRU, and FOA personnel may conduct security assistance visits upon request from the unit.

1.4.1.1. (Added-AFMC) The HQ AFMC ISPM staff will conduct a program review of each installation level ISPM security program at intervals no greater than every three years as budget allocations permit. HQ AFMC/SF will publish a schedule of planned program reviews in September for the following FY quarters. These reviews cover protection of collateral classified only. SAP and SCI classified information security programs are reviewed within their respective channels.

1.4.1.2. (Added-AFMC) The Program Review Team Leader will outbrief the CC/CV at the level of command above the ISPM at product, logistics and test centers upon completion of the review. The Team Leader will outbrief the site/organization commander, as appropriate, in all other cases. A final report will be provided within 10 working days of completion of the review.

1.4.2. Base level ISPMs will conduct program reviews on an annual basis. ***EXCEPTION:*** Conduct program reviews every two years of activities or units that do not store classified information.

1.4.2. (AFMC) Program reviews are assessments of elements of the information, personnel, industrial, safeguarding NATO and program protection security programs for policy compliance and program effectiveness. At centers, these reviews should be conducted in conjunction with reviews by

other functional security areas whenever possible to minimize impact on the organization visited. An ISPM annual program review can be counted as one semiannual self-inspection.

1.4.2.1. (Added-AFMC) Program reviews are not rated. They serve two primary purposes: (1) identify benchmark processes/products within a program for crossfeed to all serviced organizations, and (2) identify problem areas within a program and recommend corrective action. Program reviewers are encouraged to use a random sampling method; but the examination must be sufficiently thorough to determine the overall effectiveness of the program.

1.4.2.2. (Added-AFMC) Commanders and staff agency chiefs review Information Security Program Review Reports and implement corrective actions as soon as possible. This review is documented by the commander/staff agency chief endorsement to the report, with the report then filed by the security manager. Formal responses to program reviews are generally not required; however, corrective actions to remedy serious deficiencies are documented and reported according to local policy. If required by the servicing ISPM, the written response must be submitted within 30 days of notification. Keep copies of program review reports IAW records management directives. As a minimum keep a copy until the next program review report is received.

1.4.2.3. (Added-AFMC) To provide maximum flexibility consistent with a visible program, ISPMs may extend the interval between program reviews to two years when either of the following conditions exist and the delay will not affect program effectiveness. The decision to extend the frequency is reserved exclusively for the ISPM.

1.4.2.3.1. (Added-AFMC) The organization visited has relatively small classified holdings and results of other visits or inspections reflect the unit or activity has a strong information security program.

1.4.2.3.2. (Added-AFMC) The program review visit requires ISPM travel and TDY funding and budgetary constraints necessitate delaying the program review.

1.4.3. Unit commanders and equivalents involved with processing or holding classified information ensure personnel conduct semiannual security self-inspections to evaluate information security program effectiveness. ***EXCEPTION:*** Activities with a small volume of classified material may work with the ISPM to develop an oversight schedule consistent with risk management principles.

1.4.3.1. Security managers should not conduct self-inspections themselves but have others in the unit perform them.

1.5. Special Types of Information. *[Reference DoD 5200.1-R, Chapter 1, Section 3]*

1.5.1. Restricted Data. *[Reference DoDD 5210.2 and DoD 5200.1-R, Paragraph 1-300]*

1.5.1.1. General. This type of Restricted Data is described and governed by DoDD 5210.2, *Access to and Dissemination of Restricted Data*, 12 Jan 78. Air Force personnel will mark and safeguard Restricted Data according to DoDD 5210.2. Air Force certifying officials are listed in Attachment 2. These officials are responsible for certifying access to Restricted Data using DoE Form 5631.20, **Request for Visit or Access Approval** (see paragraph 5.7.1.2.). They may delegate this authority to the level they deem necessary for operational efficiency. Officials delegated the authority will sign "For" the access granting official as identified in **Attachment 2**. Air Force personnel may obtain DoE Forms 5631.20 from the DoE activity they are visiting.

1.5.1.1. (AFMC) HQ AFMC/CV, and other commanders, Program Managers and 2-Ltr Staff Agency Chiefs who report directly to the HQ AFMC Commander, are delegated this authority.

1.5.1.1.1. Activities must notify HQ USAF/XOFI through command ISPM channels of changes to the list of certifying officials (**Attachment 2**) as they occur. When doing so, they must also provide the position title, activity and office symbol of the affected party. ***NOTE:*** When the change involves an activity name change, access granting officials will sign forms authorizing access using the current activity name and a note that identifies the activity it superseded until the list of officials is updated.

1.5.1.1.2. MAJCOM, DRU, and FOA ISPMs maintain a list of certifying officials and their designees who can sign these requests. ISPMs must notify HQ USAF/XOFI of any changes to the list. HQ USAF/XOFI will periodically update a master list (**Attachment 2**) and distribute it to DoE and MAJCOM, DRU, and FOA ISPMs for their information.

1.5.1.2. Critical Nuclear Weapon Design Information (CNWDI). This type of Restricted Data is particularly sensitive and access is limited to the minimum number of people who need it to do their job.

1.5.1.2.1. CNWDI Approving Officials. These officials are responsible for granting CNWDI access. This authority is assigned to division chiefs and above at all levels of command.

1.5.1.2.1. (AFMC) Within AFMC this means 2-Ltr Directors or Staff Agency Chiefs or higher at all levels of command and commanders of all other subordinate activities and detachments.

1.5.1.3. Granting Access. Approving officials will ensure access and briefings are documented on AF Form 2583, **Request for Personnel Security Action** (available on the Air Force Electronics Publications Library (AFEPL)).

1.5.1.4. Protection. Air Force personnel will protect CNWDI in the same manner prescribed for collateral classified information. This includes limiting access to containers storing CNWDI to only those personnel who have been granted CNWDI access. *[Reference DoD 5200.1-R, Chapter 1, Section 3]*

1.5.2. North Atlantic Treaty Organization (NATO). *[Reference DoD 5200.1-R, Paragraph 1-303]*

1.5.2.1. HQ USAF/XOFI is responsible for overall development, approval, and implementation of NATO security policy within the Air Force.

1.5.2.2. HQ USAFE/SF is responsible for developing and recommending NATO security policy for implementation within the Air Force.

1.5.2.3. (Added-AFMC) The ISPM at HQ AFMC and AFMC Centers are responsible for policy and oversight of NATO security at their level.

1.6. Exceptional Situations.

1.6.1. Request for Waivers. Commanders send requests to waive provisions of AFPD 31-4, DoD 5200.1-R, or this AFI through command ISPM channels to HQ USAF/XOFI. FOAs also coordinate their requests with their respective functional head of secretariat or air staff office. *[Reference DoD 5200.1-R, Chapter 1, Section 4]*

1.6.1. (AFMC) HQ AFMC/SF is the approval authority for waivering requirements established in this supplement. Submit requests through the servicing ISPM to HQ AFMC/SF.

1.6.2. (Added-AFMC) Use AF Form 116, **Request for Deviation from Security Criteria**, to document all deviations. Consolidate multiple deviations caused by a single deficiency on one AF Form 116.

1.6.3. (Added-AFMC) The responsible activity must implement supplemental controls/compensatory measures for all temporary and permanent deviations. Activities may not use blanket waivers for several different deficiencies.

1.6.4. (Added-AFMC) The responsible/owning activity commander or two letter staff agency chief signs the 116 and submits the request to the servicing ISPM. ISPMs at all levels approve/disapprove waivers to policies contained in their implementing directives. Requests for waivers to DoD 5200.1-R requirements are forwarded through ISPM channels to the ASD(C3I) for approval/disapproval. ISPMs at each level below the approval authority review the request and add their concurrence/nonconcurrence with comments. Activities may submit three kinds of requests:

1.6.4.1.(Added). Temporary deviations (waivers) for 1 year or less. (Waiver: The approved continuance of a temporary condition that varies from an Information Security Program requirement.)

1.6.4.2. (Added-AFMC) Permanent deviations (exceptions) for a 2 year period. (Exception: The approved continuance of a non-correctable condition that varies from an information security program requirement.)

1.6.4.3. (Added-AFMC) Technical deviations (variances) for an indefinite period. (Variance: The continuance of a nonstandard condition, which technically varies from an information security program requirement, but provides essentially the same level of protection.)

1.6.6. (Added-AFMC) Supplementary Controls/Compensatory Measures compensate for the specific vulnerability created by the deficiency. These controls/measures may cover:

1.6.6.1. (Added-AFMC) Continuous protection by cleared guard or duty personnel.

1.6.6.2. (Added-AFMC) Random inspection by cleared guard or duty personnel as prescribed in DoD 5200.1-R, Section 4

1.6.6.3. (Added-AFMC) An IDS with response capability as prescribed in DoD 5200.1-R, Section 4.

1.7. Reporting Requirements. *[Reference DoD 5200.1-R, Paragraph 1-600]*

1.7.1. MAJCOM, FOA, and DRU ISPMs will submit the SF Form 311, **Agency Information Security Program Data** (available at http://www.gsa.gov/forms), report to HQ USAF/XOFI. HQ USAF/XOFI will tell ISPMs when to submit them. Interagency Report Control Number 0230-GSA-AN applies to this information collection requirement.

1.7.2. Management Information System (MIS) Reporting. AFPD 31-4 requires all activities to send their measurement data, through command ISPM channels, to HQ USAF/XOFI via Report Control Symbol (RCS): HAF-SFI(SA)9222, *The Information Security Measurement Report*. *[Reference AFPD 31-4]*

1.7.2. (AFMC) See paragraph 9.2.7(Added) and Attachment 4, A4.6.4 this supplement. ISPMs must continually strive to reduce cost and improve performance. ISPMs develop cost and performance measurements to evaluate their functional area business processes and track process changes to determine their impact on cost and effectiveness.

1.8. Administrative Sanctions.

1.8.1. Send reports through command ISPM channels to HQ USAF/XOFI when someone knowingly, willfully, or negligently discloses classified information to unauthorized individuals as specified in EO 12958. *[Reference DoD 5200.1-R, Chapter 1, Section 5]*

1.8.1. (Added-AFMC) Servicing ISPMs are responsible for forwarding reports involving collateral classified information. When these incidents involve SCI or SAP information, the servicing ISPM coordinates with the SSO or SAP office exercising oversight to ensure they are aware of the incident. It is then the responsibility of these SCI/SAP offices to forward the appropriate report through their respective program channels.

1.8.2. Air Force commanders and staff agency chiefs report unauthorized disclosures of classified information that violate criminal statutes to their servicing ISPM and Air Force Office of Special Investigations (AFOSI) offices. *[Reference DoD 5200.1-R, Chapter 1, Section 5]*

1.9. Self-Inspection. See paragraph **1.4.** of this AFI *[Reference DoD 5200.1-R, Chapter 1, Section 7]*.

1.10. Forms Prescribed. These forms are prescribed throughout this AFI and are available through the Air Force Publications Distribution system: AF Form 54, **Classified Computer Deck Cover Sheet**; AF Form 143, **Top Secret Register Page**; AF Form 144, **Top Secret Access Record and Cover Sheet**; AF Form 310, **Document Receipt and Destruction Certificate**; AF Form 1565, **Entry, Receipt, and Destruction Certificate**; AF Form 2587, **Security Termination Statement**; and, AF Form 2595, **Classified Protection Insertion Sheet.**

Chapter 2

ORIGINAL CLASSIFICATION

2.1. Original Classification Authority: *[Reference DoD 5200.1-R, Chapter 2, Section 2]*

2.1.1. The Secretary of the Air Force serves as the original classification authority (OCA) and may further delegate this authority.

2.1.2. The process for delegating OCA authority is as follows:

2.1.2.1. Secretary of the Air Force delegates Top Secret, Secret, and Confidential authority.

2.1.2.2. The Administrative Assistant to the Secretary of the Air Force delegates Secret and Confidential authority.

2.1.2.3. All requests for the delegation of original classification authority will be forwarded through command ISPM channels to the Chief, Information Security Division, HQ USAF/XOFI, 1340 Air Force Pentagon, Washington, DC 20330-1340, for processing.

2.1.2.3. (AFMC) Organizations submit requests for delegation of original classification authority through the servicing ISPM office.

2.1.2.3.1. Address requests for original Top Secret authority to the Secretary of the Air Force.

2.1.2.3.2. Address requests for original Secret and Confidential authority to the Administrative Assistant to the Secretary of the Air Force.

2.1.2.4. All requests will contain the full position title, functional office symbol, and a detailed explanation of why the position requires original classification authority.

2.1.2.5. (Added-AFMC) OCA is delegated to the position. Anyone legally assuming a designated OCA position during the temporary absence of the formally assigned occupant also assumes the OCA.

2.1.2.6. (Added-AFMC) An individual occupying a position designated OCA cannot further delegate that OCA.

2.1.3. HQ USAF/XOFI will maintain the master list of Air Force OCAs. Annually, HQ USAF/XOFI will request OCA validation from the MAJCOMs, FOAs, and DRU ISPMs. Also, submit requests for changes or new requests through command ISPM channels as they occur. See paragraph **8.5.** for training requirements.

2.1.3. (AFMC) See attachment 1 for a listing of AFMC positions with original classification authority (OCA).

2.2. Classification Prohibitions and Limitations

2.2.1. The OCA having jurisdiction over the subject matter determines if information requested under the Freedom of Information Act (FOIA) or the mandatory declassification review provisions of E.O. 12958 should be declassified. *[Reference DoD 5200.1-R, Paragraph 2-402e]*

2.3. Classification Challenges. *[Reference DoD 5200.1-R, Chapter 4, Section 9]*

2.3.1. Send challenges to classification of Air Force information, in writing, to the OCA with jurisdiction over the information in question.

2.3.1. (AFMC) Send an information copy of the challenge through the servicing ISPM to HQ AFMC/SF.

2.3.1.1. The OCA will monitor, record, and resolve all challenges to classification decisions.

2.3.1.2. Challenges to classification decisions will be processed separate from all Freedom of Information (FOIA) and Privacy Act (PA) requests unless the challenger specifically cites these authorities for obtaining the information.

2.3.2. Send challenges to classification of non-Air Force originated information, in writing, to the OCA with jurisdiction over the information in question with an information copy to HQ USAF/XOFI. This office will assist in the coordination process.

2.3.2. (AFMC) Send an information copy of the challenge through the servicing ISPM to HQ AFMC/SF.

2.3.3. Challenges to reclassification decisions are sent through command ISPM channels to HQ USAF/XOFI.

2.3.3. (AFMC) In all instances of challenges alleging underclassification, safeguard the information at the higher level of classification pending final determination. In all instances of challenges alleging overclassification, safeguard the information at the assigned level until the challenge is resolved.

2.3.4. All classified information undergoing a challenge or a subsequent appeal will remain classified until a final resolution is reached.

2.4. Classification Guides. OCAs are to publish classification guides to facilitate the proper and uniform derivative classification of their information. *NOTE:* In some cases, OCAs may determine that publishing classification guidance in other forms is more effective, i.e., program protection plans, system protect guides, Air Force instructions. In these cases, the applicable publication will be considered the guide and the reporting requirements in paragraph **2.4.2.** still apply. *[Reference DoD 5200.1-R, Chapter 2, Section 5]*

2.4.1. The responsible OCA will ensure the guide is current and reflects accurate classification instructions at all times. All guides will be reviewed at least once every two years.

2.4.2. The OCA will report publication of or changes to security classification guides to the Administrator, Defense Technical Information Center (DTIC) using Department of Defense (DD) Form 2024, **DoD Security Classification Guide Data Elements** (available at http://web1.whs.osd.mil/icdhome/DDEFORMS.HTM) and to HQ USAF/XOFI. OCAs must also forward a copy of the applicable publication or change to *[Reference DoD 5200.1-R, Paragraph 2-502e]*:

2.4.2.1. HQ USAF/XOFI, 1340 Air Force Pentagon, Washington DC 20330-1340.

2.4.2.2. AFDO, 2221 South Clark Street, Suite 600, Arlington VA 22202.

2.4.2.3. HQ AFHRA/RSA, 600 Chennault Circle, Maxwell AFB AL 36112.

2.4.2.4. (Added-AFMC) HQ AFMC/SFXP; Building 266, Room N208; 4225 Logistics Ave, Wright-Patterson AFB OH 45433-5760.

2.4.3. Within 180 days of the publication of this AFI, each OCA will provide an electronic version of their classification guidance (i.e., Security Classification Guides (SCGs), AFIs, Correspondence) for incorporation into the Air Force Electronic Publications Library. This will facilitate the development of an interactive, key word searchable database. Send a copy of the electronic version to those activities listed under paragraph **2.4.2.** if it hasn't already been done.

2.4.3. (AFMC) Forward an electronic copy to HQ AFMC/SF within 90 days of the publication of this supplement.

2.4.4. HQ USAF/XOFI will maintain the master list of all Air Force classification guides.

2.4.5. (Added-AFMC) See attachment 2 for additional guidance.

Chapter 3

DECLASSIFYING AND DOWNGRADING INFORMATION

3.1. Declassification and Downgrading Officials. Within the Air Force the following positions have been delegated the authority to declassify or downgrade classified information. This authority extends to information for which the specific declassification official has classification, program, or functional responsibility. *[Reference DoD 5200.1-R, Chapter 4, Section 1]*

3.1. (AFMC) This authority cannot be further delegated.

3.1.1. All Air Force Original Classification Authorities.

3.1.2. SAF/PAS. Chief, Office for Security Review, Office of Public Affairs, Office of the Secretary of the Air Force, 1690 Air Force Pentagon, Washington, DC, 20330-1690. See AFI 31-205, *Air Force Security and Policy Review Program*, for guidance on use of this authority.

3.1.3. HQ USAF/XOFI. Chief, Information Security Division, Directorate of Security Forces, 1340 Air Force Pentagon, Washington, DC 20330-1340.

3.1.4. AFDO, Chief, Reserve Declassification Team, 2221 South Clark Street, Suite 600, Arlington VA 22202. This authority is delegated to AFDO on a case-by-case basis by SAF/AA.

3.1.5. AFHSO/CC. Commander, Air Force History Support Office, 500 Duncan Avenue, Box 94, Bolling AFB DC 20332-1111. This authority only applies to historical documents under the jurisdiction of HQ USAF/HO and after obtaining classification recommendations from the functional owners of the information.

3.1.6. AFHRA/CC. Commander, Air Force Historical Research Agency, 600 Chennault Circle, Maxwell AFB, AL, 36112-6424. This authority only applies to historical documents under the jurisdiction of HQ USAF/HO and after obtaining classification recommendations from the functional owners of the information.

3.2. Automatic Declassification. All Air Force activities that possess classified information which is 25 years old or older and has been declared to be of permanent historical value must perform declassification reviews on the information before 15 April 2000. *[Reference DoD 5200.1-R, Chapter 4, Section 3]*

3.2.1. The Air Force Twenty Five Year Automatic Declassification Plan provides specific policy and guidance on performing automatic declassification reviews within the Air Force. See **Attachment 4**.

3.2.2. The process of automatic declassification will evolve into systematic declassification after April 2000. New guidance will be published prior to that date. For planning purposes, it is the intent of the Air Force to declassify all permanently valuable records prior to accessioning them to the National Archives.

3.3. Mandatory Declassification.

3.3.1. Send all requests for mandatory declassification review (MDR) to 11 CS/SCSR (MDR), 1000 Air Force Pentagon, Washington DC 20330-1000

3.3.1. (AFMC) Normally, the 11 CS/SCSR (MDR) forwards MDRs involving collateral classified information directly to the ISPM office servicing the OCA involved. When the 11 CS/SCSR cannot readily determine the appropriate OCA, they forward the MDR to HQ AFMC/SF for further distribu-

tion determination. HQ AFMC/SF forwards the MDR to the servicing ISPM with distribution instructions and a suspense. This suspense will normally be 10 working days after receipt. The servicing ISPM provides classification management assistance as requested by the OCA conducting the MDR. MDRs involving SCI or SAP information are handled through those program channels.

3.3.2. Send appeals to MDR decisions through 11 CS/SCSR (MDR) to SAF/AA, the Air Force Appellate Authority for MDRs.

Chapter 4

MARKING

Section 4A—General Provisions

4.1. General. Air Force personnel who originally and derivatively classify information will mark those products according to DoD 5200.1-R. They may also use DoD 5200.1-PH, *Marking Classified Documents,* to guide them through the process. *[Reference DoD 5200.1-R, Chapter 5, Section 1]*

Section 4B—Specific Markings on Documents [Reference DoD 5200.1-R, Chapter 5, Section 2]

4.2. Reason for Classification. In the case of exempted information, the reason(s) for classification must be consistent with the exemption category(ies). *[Reference DoD 5200.1-R, Paragraph 5-203]*

4.3. Declassification Instructions. The exemption category(ies) must be consistent with the reason(s) used for classifying the information. *[Reference DoD 5200.1-R, Paragraph 5-204]*

4.4. Marking Waivers. Requesters send requests for marking waivers through command ISPM channels to HQ USAF/XOFI. For Special Access Program (SAP) marking requirements, send requests through command SAP channels to SAF/AAZ. *[Reference DoD 5200.1-R, Paragraph 5-206d]*

4.5. Special Control and Similar Notices. *[Reference DoD 5200.1-R, Paragraph 5-208]*

4.5.1. Communications Security (COMSEC). See AFI 33-211, *Communications Security (COMSEC) User Requirements,* for additional guidance on marking COMSEC media. *[Reference DoD 5200.1-R, Paragraph 5-208d]*

4.5.2. Technical Documents. See AFI 61-204, *Disseminating Scientific and Technical Information,* for guidance on disseminating technical documents. *[Reference DoD 5200.1-R, Paragraph 5-208e]*

4.5.3. SAPs. See AFI 16-701, *Special Access Programs,* for additional guidance on SAP documents. *[Reference DoD 5200.1-R, Paragraph 5-208f]*

4.5.4. Other Special Notices. See **Attachment 2** for references. *[Reference DoD 5200.1-R, Paragraph 5-208h]*

4.6. Removable AIS Storage Media. Personnel use SF Form 706, **Top Secret ADP Media Classification Label**; SF Form 707, **Secret ADP Media Classification Label**; SF Form 708, **Confidential ADP Media Classification Label**; and, SF Form 711, **ADP Data Descriptor Label**, on removable AIS storage media. These are available through the Air Force Publications Distribution system. *[Reference DoD 5200.1-R, Paragraphs 5-407 and 5-409a-b]*

4.7. Intelligence. *[Reference DoD 5200.1-R, Paragraph 5-410]*

4.7.1. See AFI 14-302, *Control, Protection, and Dissemination of Sensitive Compartmented Information,* for Air Force policy on intelligence. *[Reference DoD 5200.1-R, Paragraphs 5-410a-b]*

4.7.2. The Special Security Office (SSO) is the focal point for release and dissemination of SCI. The Director of Central Intelligence Directive 5/6, *Intelligence Disclosure Policy*, provides criteria for release of intelligence to foreign officials. *[Reference DoD 5200.1-R, Paragraph 5-410c]*

4.8. (Added-AFMC) The absence of "NOFORN," or equivalent markings is not authority for any release to a foreign government, representative thereof, or international organization. This applies to classified national security information and unclassified controlled information, but not to information approved for public release. Contact the designated Foreign Disclosure Office for applicable Delegated Disclosure Lists (DDL).

4.9. (Added-AFMC) The last page of a document will be considered its back cover unless there is a clearly discernible separate page serving as the cover. Mark the back cover as required in the basic directive.

4.10. (Added-AFMC) Mark file folders containing classified information on the top and bottom of the front and back of the folder with the highest level of classified material contained therein.

Chapter 5

SAFEGUARDING

Section 5A—Control Measures

5.1. General. The Air Force will control and account for classified information as described in paragraph **5.11.** of this instruction. *[Reference DoD 5200.1-R, Paragraph 6-100a]*

5.2. Reserve Component Participation In Security Planning. Reserve components should be included early on in the security planning phase for weapon systems that will be directly released to and operated by reserve forces.

5.3. Working Papers. Originators must also show their name, organization, and office symbol on classified working papers in indelible ink. *[Reference DoD 5200.1-R, Paragraph 6-101]*

Section 5B—Access

5.4. Granting Access to Classified Information. Personnel who have authorized possession, knowledge, or control of classified information grant individuals access to classified information when required for mission essential needs and when the individual has the appropriate access level according to AFI 31-501; has signed an SF 312, **Classified Information Nondisclosure Agreement** (available on the AFEPL); and, has a need to know the information. Those granting access to classified information must gain the originator's approval before releasing the information outside the Air Force or as specified by the originator of the material. Also see paragraph **5.6.1.1.** of this AFI. *[References DoD 5200.1-R, Paragraph 6-200, and EO 12958, Section 4.2(b)]*

5.4.1. Confirm an Individual's Access Level. Those granting access to classified information will confirm a person's access level by:

5.4.1.1. Checking the person's access level on the Automated Security Clearance Approval System (ASCAS) roster or Sentinel Key (ASCAS successor) clearance record. This only applies to Air Force employees (See AFI 31-501);

5.4.1.2. Confirming it through the employee's security manager, supervisor, or commander;

5.4.1.3. Checking the access level on a person's temporary duty (TDY) or permanent change of station (PCS) orders; or,

5.4.1.4. Receiving a visit request from the visitor's security manager or supervisor. See paragraph **5.7.2.** for further guidance.

5.5. Nondisclosure Agreement (NdA). Signing the NdA is a pre-requisite for obtaining access (see paragraph **5.4.**). Unit commanders, staff agency chiefs, or designated personnel are responsible for ensuring their employees have signed one by checking the Automated Security Clearance Approval System (ASCAS) or the employee's personnel records. If they have not signed one, those responsible use DoD 5200.1-PH-1, *Classified Information Nondisclosure Agreement (Standard Form 312) Briefing Pamphlet*, to brief people on the purpose. Also see DoD 5200.1-R, paragraph 9-200b for training requirements.

NOTE: When the employee's access level is passed to another office or activity, that office or activity can assume the employee has signed one.

5.5.1. Retention. The following organizations will retain NdAs for 50 years.

5.5.1.1. For active military members, security managers send NdAs to HQ AFPC/DPSRI1, 550 C St., W, Suite 21, Randolph AFB, TX 78150-4723.

5.5.1.2. For reservists, security managers send NdAs to HQ ARPC/DSMPM, 6760 E. Irvington Place, #4450, Denver, CO 80280-4450.

5.5.1.3. For retired general officers receiving access under the provisions of AFI 31-501 and who do not already have a signed NdA in their retired file, ISPMs send NdAs to HQ AFPC/DPSRS, 550 C St., W, Suite 21, Randolph AFB TX 78150-4723.

5.5.1.4. For Air Force civilians, the servicing civilian personnel office files the NdA in the person's official personnel file.

5.5.1.5. For persons outside the Executive Branch who receive access according to paragraph **5.6.**, the servicing ISPM to the activity granting access will file the NdA. They must retain them for 50 years.

5.5.2. When To Sign.

5.5.2.1. Unit commanders and staff agency chiefs may allow their people 30 days to sign a NdA.

5.5.2.2. Air Reserve and the Guard may allow their people eight training days to sign.

5.5.3. Refusal To Sign. When a person refuses to sign a NdA, the commander:

5.5.3.1. Records the fact the person refused to sign it.

5.5.3.2. Denies the individual access to classified information.

5.5.3.3. Takes steps to deny or revoke the person's security clearance eligibility by setting up a Security Information File according to AFI 31-501.

5.6. Access by Persons Outside the Executive Branch.

5.6.1. Policy. MAJCOM, DRU, and FOA commanders and heads of Secretariat or Air Staff offices or their designees authorize individuals outside the executive branch to access Air Force classified material as follows unless otherwise provided in DoD 5200.1-R, paragraph 6-201. *[Reference DoD 5200.1-R, Paragraph 6-201]*

5.6.1.1. Authorizing Officials (those cited in paragraph **5.6.1.** above) may grant access once they have:

5.6.1.1.1. Gained release approval from the originator or owner of the information.

5.6.1.1.2. Determined the individual has a current favorable personnel security investigation as defined by AFI 31-501 and a check of the Defense Clearance and Investigations Index (DCII) and a local files check (LFC) shows there is no unfavorable information since the previous clearance. A LFC must be processed according to AFI 31-501. ***EXCEPTION:*** In cases where there is no current personnel security investigation as defined in AFI 31-501, MAJCOM, DRU, and FOA commanders and heads of Secretariat or Air Staff offices may request a National Agency Check (NAC) and grant access up to the Secret level before the NAC is

complete when there is a favorable LFC and the 497 IG/INS confirms there is no unfavorable information on the individual in the DCII.

5.6.1.1.3. Determined granting access will benefit the government.

5.6.1.2. Requests for access must include:

5.6.1.2. (AFMC) Requests for access must be signed by a Commander, Special Program Office Director, or 2-Ltr Staff Agency Chief/Director or higher, and be submitted 120 days prior to required access. This permits time for requesting and completing the appropriate background investigation.

5.6.1.2.1. The person's name, date and place of birth, and citizenship.

5.6.1.2.2. Place of employment.

5.6.1.2.3. Name and location of installation or activity where the person needs access.

5.6.1.2.4. Level of access required.

5.6.1.2.5. Subject of information the person will access.

5.6.1.2.6. Full justification for disclosing classified information to the person.

5.6.1.2.7. Comments regarding benefits the U.S. Government may expect by approving the request.

5.6.1.3. The authorizing official will coordinate the processing of the NAC request with the nearest Air Force authorized requester of investigations.

5.6.1.4. Individuals with approval must sign a NdA before accessing information. Upon completion of access, individuals must sign an AF Form 2587, **Security Termination Statement**.

5.6.2. Congress. See AFI 90-401, *Air Force Relations with Congress*, for guidance when granting classified access to members of Congress, its committees, members, and staff representatives. *[Reference DoD 5200.1-R, Paragraph 6-201a]*

5.6.3. Government Printing Office (GPO). The GPO processes and confirms their personnel's access. *[Reference DoD 5200.1-R, Paragraph 6-201b]*

5.6.4. Representatives of the General Accounting Office (GAO). See AFI 65-401, *Relations with the General Accounting Office*, for access requirements. *[Reference DoD 5200.1-R, Paragraph 6-201c]*

5.6.5. Historical Researchers. AFHSO is the authority for granting access to historical researchers on behalf of the Air Force Historian (HQ USAF/HO). *[Reference DoD 5200.1-R, Paragraph 6-201d]*

5.6.5.1. General. Requests for classified access by historical researchers will be processed only in exceptional cases wherein extraordinary justification exists. Access will be granted to the researcher only if the records cannot be obtained through available declassification processes (i.e., the FOIA and MDR processes) and when the access clearly supports the interests of national security.

5.6.5.2. Providing Access.

5.6.5.2.1. The researcher must apply to AFHSO in writing for the access. The application will fully describe the project including the sources of documentation that the researcher wants to access.

5.6.5.2.2. If AFHSO accepts the request for access, they will provide the researcher with written authorization to go to the nearest Air Force installation security office to fill out the necessary paperwork for a national agency check (NAC) according to AFI 31-501.

5.6.5.2.3. If the results of the NAC are favorable and AFHSO approves access, the researcher must sign a SF 312 and an agreement to submit any notes and manuscript(s) for security and policy review (AFI 35-205, *Air Force Security and Policy Review Program*). This process is to ensure the documents do not contain any classified information and, if so, determine if they can be declassified. Send the SF 312 to AFHSO for retention.

5.6.5.2.4. Other Terms.

5.6.5.2.4.1. The access agreement is valid for two years. One two-year renewal is possible. A renewal will not be considered if the project appears to be inactive in the months before the end of the original agreement.

5.6.5.2.4.2. Access will be limited to those records 25 or more years of age.

5.6.5.2.4.3. Access based on a NAC is good for Secret and Confidential information but does not meet the requirement for access to Restricted Data (RD) or SAP information. Access to Top Secret information is not authorized.

5.6.5.2.4.4. Access will be allowed only to Air Force records at AFHSO, AFHRA, and the National Archives and Records Administration (NARA).

5.6.5.2.4.5. Access to Air Force records still in the custody of the originating offices in the Washington National Capital Region must be approved in writing by the originating offices or their successors. It is the responsibility of the researcher to secure this approval.

5.6.6. Former Presidential Appointees. Persons who previously occupied policy making positions to which they were appointed by the President may not remove classified information upon departure from office. All such material must remain under the security control of the U.S. Government. Such persons may be authorized access to classified information they originated, received, reviewed, signed, or that was addressed to them while serving in their official capacity, provided the applicable Air Force original classification authority: *[Reference DoD 5200.1-R, Paragraph 6-201e]*

5.6.6.1. Makes a written determination that such access is clearly consistent with the interests of national security;

5.6.6.2. Uses the same access determination procedures outlined in paragraph **5.6.1.1.** of this AFI;

5.6.6.3. Limits the access to specific categories of information over which the Air Force original classification authority has classification jurisdiction;

5.6.6.4. Maintains custody of the information or authorizes access to documents in the custody of the NARA; and,

5.6.6.5. Obtains the individual's agreement to safeguard the information and to submit any notes and manuscript for a security review (AFI 35-205) to ensure that the documents do not contain classified information or to determine if any classified information should be declassified.

5.6.7. Judicial Proceedings. See AFI 51-301, *Civil Litigation*, for more information regarding the release of classified information in litigation.

5.6.8. Other Situations. Follow the guidance in paragraph **5.6.1.1.** above. *[Reference DoD 5200.1-R, Paragraph 6-201g]*

5.6.9. Foreign Nationals, Foreign Governments, and International Organizations. Owners of classified information disclose it to foreign nationals, foreign governments, and international organizations only when they receive authorization from SAF/IAD, 1080 Air Force Pentagon, Washington DC 20330-1080. (See AFI 16-201, *Foreign Disclosure of Classified and Unclassified Military Information to Foreign Governments and International Organizations*, for more specific guidance.)

5.6.10. Retired Flag or General Officers or Civilian Equivalent. See AFI 31-501. These individuals need not sign a NdA if the original one is already filed in their retired file (see paragraph **5.5.1.3.**).

5.7. Access by Visitors. *[Reference DoD 5200.1-R, Paragraph 6-202]*

5.7. (AFMC) Servicing ISPMs must incorporate visitor control policies and procedures in their local supplement to this directive. These must, as a minimum, define local processes for sending and receiving visit requests, evaluating visit requests, controlling visitors during the visit, tracking the visit to ensure timely departure of visitors, and maintenance of visitor record files. Visit records involving foreign national access to classified or controlled unclassified information must be maintained for a minimum of two years following expiration of the visit or as specified in AFMAN 37-139, *Records Disposition Schedule*. This requirement does not supplant, mitigate or otherwise impact foreign disclosure policies/ requirements regarding foreign national visitors.

5.7.1. Outgoing Visit Requests for Air Force Employees. When an Air Force employee requires access to classified information at:

5.7.1.1. A contractor activity, the supervisor or security manager forwards a visit request to the contractor's visitor control center or facility security office. The visit request will include the same information required by DoD 5220.22-M, *National Industrial Security Program Operating Manual*, Jan 95.

5.7.1.2. A Department of Energy (DoE) activity, the supervisor or security manager prepares and processes DoE Form 5631.20, **Request for Visit or Access Approval**, according to DoDD 5210.2, *Access to and Dissemination of Restricted Data*. Also see paragraph **1.5.1.1.** of this AFI.

5.7.1.3. Another Air Force activity, see paragraph **5.4.1.**

5.7.1.4. Another agency, the supervisor or security manager forwards a visit request to the agency security office unless instructed otherwise.

5.7.1.5. (Added-AFMC) Unless otherwise specified, the visit request will, as a minimum, include the name and citizenship of the visitor, the visitor's organization and telephone number, certification of the visitor's clearance and any special access authorizations required for the visit, the name of person(s) to be visited, and the purpose and date or period of the visit. AF Form 97 can be used for providing visit notices.

5.7.2. Incoming Visit Requests. Air Force activity visit hosts serve as the approval authority for visits to their activities. Installation or activity commanders receiving a visit request:

5.7.2.1. From Air Force employees, see paragraph **5.4.1.**

5.7.2.2. From contractors, see DoD 5220.22-M, Chapter 6.

5.7.2.3. From foreign nationals or U.S. citizens representing a foreign government, commanders or their designees process the visit request according to AFI 16-201.

5.7.3. Duration of Visit Request. Visit requests are valid for up to a year—renew them annually as necessary to accomplish the mission.

5.8. Preventing Publication of Classified Information in the Public. See AFI 35-205 for guidance on security reviews to keep people from publishing classified information in personal or commercial articles, presentations, theses, books or other products written for general publication or distribution.

5.9. Access to Information Originating in a Non-DoD Department or Agency. Holders allow access under the rules of the originating agency.

5.10. Administrative Controls.

5.10.1. Top Secret. The Air Force accounts for Top Secret material and disposes of such administrative records according to AFMAN 37-139. These procedures ensure stringent need to know rules and security safeguards are applied to our most critical and sensitive information.

5.10.1.1. Establishing a Top Secret Control Account (TSCA). Unit commanders and staff agency chiefs who routinely originate, store, receive, or dispatch Top Secret material establish a Top Secret account and designate a Top Secret Control Officer (TSCO), with one or more alternates, to maintain it. The TSCO uses AF Form 143, **Top Secret Register Page**, to account for each document (to include page changes and inserts) and each piece of material or equipment to include Automated Information System (AIS) media. ***NOTE:*** For AIS or microfiche media, TSCOs must either describe each Top Secret document stored on the media on the AF Form 143 or attach a list of the documents to it. This will facilitate a damage assessment if the media is lost or stolen. ***EXCEPTIONS:***

5.10.1.1.1. Top Secret Messages. TSCOs don't use AF Form 143 for Top Secret messages kept in telecommunications facilities on a transitory basis for less than 30 days. Instead, use message delivery registers or other similar records of accountability.

5.10.1.1.1. (AFMC) This includes communications centers and command posts.

5.10.1.1.2. Defense Courier Service (DCS) Receipts. TSCOs don't use AF Forms 143 as a receipt for information received from or delivered to the DCS. DCS receipts suffice for accountability purposes in these cases.

NOTE:

TSCOs may automate their accounts as long as all of the required information is included in the AIS.

5.10.1.2. Top Secret Disclosure Records.

5.10.1.2.1. The TSCO uses AF Form 144, **Top Secret Access Record and Cover Sheet**, as the disclosure record and keeps it attached to the applicable Top Secret material.

5.10.1.2.2. People assigned to an office that processes large volumes (i.e., several hundred documents) of Top Secret material need not record who accesses the material. ***NOTE:*** This applies only when these offices limit entry to assigned and appropriately cleared personnel identified on an access roster.

5.10.1.3. Top Secret Inventories. Unit commanders and staff agency chiefs:

5.10.1.3.1. Designate officials to conduct annual inventories for all Top Secret material in the account and to conduct inventories whenever there is a change in TSCOs. These officials must be someone other than the TSCO or alternate TSCOs of the TSCA being inventoried. The purpose of the inventory is to ensure all of the Top Secret material is present and its status is correctly annotated on the AF Form 143.

5.10.1.3.2. Ensure necessary actions are taken to correct deficiencies identified in the inventory report.

5.10.1.3.3. Ensure the inventory report and a record of corrective actions taken are maintained with the account.

5.10.1.4. Top Secret Receipts. TSCOs use AF Form 143 as a receipt when transferring Top Secret material from one TSCO to another on the same installation.

5.10.1.5. Top Secret Facsimiles. Top Secret facsimiles will be processed as another copy of the main Top Secret document in the TSCA. All the same rules apply except the register page and disclosure record will be faxed along with the document to the addressee. The addressee will sign and return them immediately to the sender for inclusion in the TSCA.

5.10.1.6. (Added-AFMC) Commanders or staff agency chiefs establish TSCAs only when mission dictates, and disestablishes them when no longer required or after 12 months of no receipt, generation or storage of material. Provide written notice of TSCA establishment and closure to the local Information Management Office, when appropriate, and the servicing ISPM. Send a copy of each TSCO and alternate's written appointments to the same offices. Ensure TSCO and alternates attend training provided by the servicing ISPM.

5.10.2. Secret. Unit commanders and staff agency chiefs set up procedures for internal control of Secret material. ***NOTE:*** Personnel may use AF Form 310, **Document Receipt and Destruction Certificate**, as a receipt when transmitting Secret material. Personnel possessing Secret material must use a receipt when:

5.10.2.1. Entering Secret material into a mail distribution system.

5.10.2.2. Handcarrying Secret material off an installation (i.e., Air Force base, separately located missile field) or to non-Air Force activities.

5.10.2.3. Handcarrying Secret material to a recipient not shown on the material's distribution and who is with another DoD agency or Service or another Air Force activity residing on the same installation (i.e., the Pentagon, Air Force Base). ***EXCEPTION:*** Within the National Capital Region (NCR), a receipt is not required when transferring Secret material to an Air Force activity shown on the distribution list.

5.10.3. Confidential. Individuals need not use a receipt for Confidential material unless asked to do so by the sending activity.

5.10.4. Foreign Government Information. See DoD 5200.1-R, Chapter 6, Section 6, for receipting requirements.

5.10.5. Retention of Receipts. Retain receipt and other accountability records in accordance with AFMAN 37-139, *Records Disposition Schedule.*

Section 5C—Safeguarding

5.11. Care During Working Hours. Personnel removing classified material from storage must,

5.11.1. For Top Secret material, use AF Form 144 or AF Form 54, **Classified Computer Deck Cover Sheet**, instead of SF Form 703, **Top Secret Cover Sheet** (see paragraph 5.10.1.3.1). *[Reference DoD 5200.1-R, Paragraph 6-301]*

5.11.2. For Secret or Confidential material, use SF Form 704, **Secret Cover Sheet**, or SF Form 705, **Confidential Cover Sheet**, as appropriate. These forms are available through the Air Force Publications Distribution system.

5.12. End-of-Day Security Checks. Each unit and staff agency that processes classified information will conduct an end-of-day security check to ensure classified material is stored appropriately. Personnel conducting these checks will do so at the close of each working day and record them on the SF Form 701, **Activity Security Checklist**, and the SF Form 702**, Security Container Check Sheet**, when security containers are present. The SF Form 701 is available on the AFEPL and the SF Form 702 is available through the Air Force Publications Distribution system.

5.13. Residential Storage Arrangements.

5.13.1. SAF/OS and SAF/AA authorize the removal of Top Secret information from designated working areas in off-duty hours for work at home. Requesters send requests through command ISPM channels to HQ USAF/XOFI. ***[Reference DoD 5200.1-R, Paragraph 6-306a]***

5.13.2. MAJCOM, FOA, and DRU commanders, or their ISPMs approve requests for removing Secret and Confidential material from designated work areas during non-duty hours. *[Reference DoD 5200.1-R, Paragraph 6-306b]*

5.13.2. (AFMC) All AFMC General Officers may take Secret and Confidential classified national security information to their home for work purposes provided they reside on a base with an access controlled perimeter and have an approved GSA security container in their residence. The combination to the residence container must be stored in an approved GSA container within the Commander's work center to permit retrieval of the container's contents in the event of an emergency. This authorization does not apply to caveated information such as SCI, SAR, NATO, etc. In all other cases submit requests through the servicing ISPM office to HQ AFMC/SF. The servicing ISPM reviews the request and recommends approval/disapproval. HQ AFMC/CC has delegated final approval authority for these requests to AFMC/SF.

5.13.3. Contingency Plans. The written procedures will include arrangements for notifying the responsible activity to pick up the classified container and material in the event something happens to the user. *[Reference DoD 5200.1-R, Paragraph 6-306c]*

5.14. In-Transit Storage. Installation commanders

5.14.1. Provide an overnight repository for classified material and ensure operations dispatch, passenger services, base entry controllers, and billeting people know about it.

5.14.1. (AFMC) Cargo security cages or rooms used for temporary storage of classified material must have an intrusion detection alarm operating when attendants are not present. Servicing ISPMs must review and approve these areas prior to their establishment.

5.14.2. Authorize the storage of Secret material on the flightline during in-processing for deployment when the material is stored in a standard GSA approved security container setting on a pallet and the in-transit area is controlled and located on an Air Force installation.

5.14.2. (AFMC) "Controlled" means the continual presence of government military or civilian personnel in such proximity as to allow observation and controlling of access to the security container, or the area is monitored by an approved alarm system.

5.15. Classified Meetings and Conferences. *[Reference DoD 5200.1-R, Paragraph 6-307]*

5.15.1. General. Activities hosting the meetings described will ensure appropriate security measures are taken to protect classified information discussed and provided to the attendees. These activities will develop a security plan addressing how the issues discussed in DoD 5200.1-R, paragraph 6-307, will be accomplished. For science and technology related meetings, see AFI 61-205, *Sponsoring or Cosponsoring, Conducting, and Presenting DoD Related Scientific Papers at Unclassified and Classified Conferences, Symposia, and Other Similar Meetings.*

5.15.1. (AFMC) Activities hosting classified meetings will coordinate their security plan with the servicing ISPM. As a minimum, this plan should contain the meeting title, its location, purpose, classification level (if permitted), identity of the responsible security manager, and a statement of who (organization or title) approved the meeting. Also, the plan must address visit request and clearance verification procedures prior to attendee arrival, an assessment of acoustical security controls required during the meeting (e.g. perimeter guards), access controls at the meeting entry point, policy on introducing and utilization of electronic or photographic devices in the meeting room, storage of classified materials (exhibits/documents) before, during and after the meeting, policy/procedures for note-taking during classified portions of the meeting, and communications/destruction/transmission procedures for those requiring these services during or after the meeting. The plan is not limited to these areas alone and may be expanded as determined locally.

5.15.2. Approval Authority. Installation commanders or their designees assess the need to set up and approve secure conference facilities under their security control. Normally, secure conference facilities are only set up at locations where frequent classified meetings or forums occur. Since these facilities are located on Air Force installations and are not used to store classified information, secure construction requirements are not mandated. However, if installation commanders or their designees determine the local threat and security environment dictates more stringent construction requirements, they can use DoD 5200.1-R, Appendix G as a guide for constructing the facility. For guidance on classified meetings scheduled at DoD contractor facilities, see DoD 5220.22-M, and AFI 31-601, *Industrial Security Program Management.*

5.15.2. (AFMC) The servicing ISPM ensures security requirements are met by coordinating on all construction plans and procedures for secure conference rooms and by conducting a physical security survey upon completion of construction. All issues regarding EMSEC or TSCM requirements for these rooms are the responsibility of SC and OSI respectively. ISPMs shall maintain a listing of all approved secure conference rooms for customers they service.

5.15.3. Foreign Participation. Hosting officials refer to both AFI 16-201, *Foreign Disclosure of Classified and Unclassified Military Information to Foreign Governments and International Organizations,* and AFI 61-205, *Sponsoring or Cosponsoring, Conducting, and Presenting DoD Related Sci-*

entific Technical Papers at Unclassified and Classified Conferences, Symposia, and Other Similar Meetings for specific guidance.

5.15.4. Other Types. Meetings, conferences, seminars, and activities other than those described in DoD 5200.1-R, paragraph 6-307a, pertain to those that are going to be held at a non-government-owned and uncleared facility. In these cases, SAF/AA must approve the event. Hosting officials send requests through command ISPM channels to HQ USAF/XOFI. The request must include a security plan that describes how the issues discussed in DoD 5200.1-R, paragraph 6-307 will be accomplished. *[DoD 5200.1-R, Paragraph 6-307b]*

5.15.4. (AFMC) Servicing ISPMs review these requests to ensure all security requirements are satisfied and provide formal concurrence/nonoccurrence with the final security plan.

5.15.5. Technical Surveillance Countermeasures (TSCM) Surveys. Commanders or their designees determine to do TSCM surveys based on mission sensitivity and threat. See AFI 71-101, Volume I, *Criminal Investigations, Counterintelligence, and Protective Service Matters,* for additional guidance.

5.16. Protecting Classified Material on Aircraft Located in Foreign Countries.

5.16.1. General. Aircraft commanders are responsible for the protection of classified information on their aircraft when stopping in foreign countries in accordance with DoD 5200.1-R, paragraph 6-308. As such, they must plan security for these stopping points. This includes factoring in the appropriate manpower to stay with the classified material or making arrangements with the nearest U.S. Air Force unit or other U.S. Government activity for security support when needed. The planning process will also address appropriate actions to take in the event of an emergency landing. *[Reference DoD 5200.1-R, Paragraph 6-308]*

5.16.2. Investigative and Clearance Requirements for Personnel Guarding the Aircraft.

5.16.2.1. For classified equipment/material not visible from outside the aircraft, only U.S. citizens with favorable Entrance National Agency Checks or higher may watch over the aircraft and respond to emergencies. ***EXCEPTION:*** Non-U.S. citizens determined to be eligible for access to the classified equipment/material through the foreign disclosure process.

5.16.2.2. For classified equipment/material visible from the aircraft, only U.S. citizens with clearance equal to the equipment classification may watch over the aircraft or respond to emergencies. ***EXCEPTION:*** Non-U.S. citizens determined to be eligible for access to the classified equipment/material through the foreign disclosure process.

5.16.2.3. See AFI 31-501 for procedures on obtaining a personnel security investigation and clearance.

5.17. Information Processing Equipment.

5.17.1. Machines with Copying Capability. For copiers and facsimile machines or any machines with copying capability (i.e., microfiche machines), personnel consult their servicing information manager to determine if the machines are authorized for copying classified, and if so, determine if they retain any latent images when copying classified, and how to clear them when they do. When they need to be cleared, destroy the waste as classified material latent images are visible. Machine custodians must post a notice on machines approved for copying classified to inform users of the

authority and clearance procedures. Also see paragraph **5.27.** for reproduction authority. *[Reference DoD 5200.1-R, Paragraph 6-309]*

5.17.2. AIS Removable Equipment/Media.

5.17.2.1. For AIS machines and media (i.e., diskettes, compact discs) approved for processing classified information, personnel protect the AIS equipment or the removable hard disk drive and the AIS media at the protection level required by DoD 5200.1-R, Chapter 6 for the highest security classification processed by the AIS.

5.17.2.2. In the case of AIS media (i.e., diskettes, compact discs) used for storing classified information, personnel protect the media at the protection level required by DoD 5200.1-R, Chapter 6, for the highest security classification stored on the media.

5.17.3. Printer Ribbons and Toner Cartridges. For any type of printer with a ribbon that has been used to print classified information, personnel remove the ribbon and store it as classified. This also applies to printers with toner cartridges that retain latent images of the classified. See DoD 5200.1-R, Chapter 6 for storage requirements.

5.18. General Safeguarding Policy. *[Reference DoD 5200.1-R, Paragraph 6-400]*

5.18.1. See DoD 5200.1-R, paragraphs 1-400 and 6-800, when considering use of alternative safeguarding measures.

5.18.1. (AFMC) Submit requests to use alternative or compensatory security controls in protecting classified national security information to HQ AFMC/SF for approval/disapproval. In emergencies, when there is no time to first submit a request, controls are applied as deemed necessary and the request is submitted as soon as possible thereafter. This process does not replace or obviate the requirements of DoD 5200.1-R, paragraph 1-401 regarding the submission of waivers.

5.18.2. Use of Force for the Protection of Classified Material. See AFI 31-207, *Arming and Use of Force by Air Force Personnel.*

5.18.3. Sensitive Compartmented Information (SCI) Safeguarding Policy. See Air Force Manual (AFMAN) 14-304, *The Security, Use, and Dissemination of Sensitive Compartmented Information (supersedes USAFINTEL 201-1).*

5.18.4. Retention of Classified Records. Personnel follow the disposition guidance in AFMAN 37-139, *Records Disposition Schedule.*

5.19. Standards for Storage Equipment. Holders of classified material may not use containers without a General Services Administration (GSA) label. If a label is not present on the outside or in the locking drawer of the container, a locksmith should be able to confirm the safe is a GSA approved container. If there is doubt, personnel may contact the DoD Lock Hotline

(DSN 551-1212) or GSA through supply channels for assistance. Personnel must note their findings and the source of confirmation on an Air Force Technical Order (AFTO) Form 36**, Maintenance Record for Security Type Equipment** (available on the AFEPL), and retain that record in the container. *[Reference DoD 5200.1-R, Paragraph 6-401]*

5.20. Storage of Classified Information. ***[Reference DoD 5200.1-R, Paragraph 6-402]***

5.20.1. Security-In-Depth. Installation perimeter fencelines, entry control points, controlled and restricted area designations, base patrol coverage, and locked building constitute Air Force "security-in-depth" measures. *[Reference DoD 5200.1-R, Paragraph 6-402 and Appendix B]*

5.20.2. Authority for Delineating the Appropriate Security Measures. If these requirements cannot be met because of local conditions, ISPMs determine alternative methods under the provisions of DoD 5200.1-R, paragraph 6-800. Military commanders do so when it occurs during a military operation as described in DoD 5200.1-R, paragraph 1-400. *[Reference DoD 5200.1-R, Paragraph 6-402d(1)]*

5.20.2. (AFMC) Paragraph 5.18.1, this supplement, applies when ISPM approval is required.

5.20.3. Replacement of Combination Locks. Commanders must ensure all combination locks on GSA approved security containers and doors are replaced with those meeting Federal Specification FF-L-2740 starting with those storing the most sensitive information according to the priority matrix in DoD 5200.1-R, Appendix G. There is no deadline for completing this effort because when it initially started it was an unfunded requirement. However, commanders must pursue funding for it and implement the retrofits as soon as possible. Commanders must also consider the fact that a location is identified for closure when prioritizing replacement of locks on security containers. *[Reference DoD 5200.1-R, Paragraph 6-402e]*

5.20.4. (Added-AFMC) The installation commander, in concert with the servicing ISPM and base civil engineer, approves storage of classified national security information in open or unattended storage areas. This includes secure rooms on base, and off base when in the local area and under government control. The installation commander may delegate this approval authority to the servicing ISPM by incorporating such delegation into local supplementation to this directive. The base civil engineer confirms construction of the secure room is IAW DoD 5200.1-R, Appendix G. Before these areas are approved, the using commander, director or staff agency chief submits to the approving authority a written plan for utilization of the secure room, to include security controls employed to provide adequate safeguarding protection and positive entry control to the storage area. The servicing ISPM reviews this plan for accuracy and thoroughness and recommends concurrence/nonconcurrence to the approving authority. See Appendix G, DoD 5200.1-R for construction standards and procedural requirements.

5.20.5. (Added-AFMC) The purpose of a secure room is to open store classified material when the size and nature of the material, or operational necessity, make the use of General Services Administration (GSA) approved containers or vaults unsuitable or impractical. Secure rooms are never approved solely for the purpose of operational convenience or in lieu of obtaining and using otherwise appropriate GSA-approved containers. In addition, secure rooms are approved to meet a specific operational requirement and only classified national security information relative to that specific requirement should be stored in the approved room. Users of secure rooms must ensure their operational procedures comply with the spirit and intent of this purpose and avoid expedient approaches which reduce protective measures or increase the possibility of compromising classified national security information.

5.20.6. (Added-AFMC) All structures designated as secure rooms after 20 Nov 96, or new secure rooms constructed after 20 Nov 96, and storing SECRET material/information, which are not continuously occupied or guarded, will be alarmed. Secure rooms approved prior to 20 Nov 96 are exempt from this requirement; however, programming action to fund alarms for these rooms must be pursued

when feasible and must be included in any modification or rehabilitation plans. This "grandfathering" provision only applies to the current program, project or activity that necessitated establishment of the secure room. It doesn't apply to follow-on unrelated programs, projects or activities. Secure room certification is not indefinite and is applicable only for the duration of a program, project or activity and terminates upon completion of the requirement. Install and operate alarm systems IAW DoD 5200.1-R, Appendix G; AFI 31-209; and AFH 31-223, paragraph 10. Minimum system requirements are described in DoD 5200.1-R, Appendix G, Section B, paragraph 5. Submit waivers for alarm requirements to HQ AFMC/SF, through the servicing ISPM, following procedures contained in paragraphs 1.6.1. through 1.6.6.3. above.

5.20.7. (Added-AFMC) Servicing ISPMs maintain records of all secure rooms to include the specific location of the room, certification of compliance with construction requirements, and approval for the current occupant to operate the secure room. Provide the following information to HQ AFMC/SFXP NLT 31 Jan of each calendar year: Number of secure rooms on the installation, number alarmed, number established as long term and number established as short term. Long term is defined as greater than 12 months. ISPMs develop local procedures to establish this baseline and track compliance.

5.21. Use of Key Operated Locks. *[Reference DoD 5200.1-R, Paragraph 6-402f(1)]*

5.21.1. The authority to determine the appropriateness of using key operated locks for storage areas containing bulky Secret and Confidential material is delegated to the chief of the activity having this storage requirement. When key operated locks are used, the authorizing official will designate lock and key custodians.

5.21.2. Lock and key custodians use AF Form 2427, **Lock and Key Control Register** (available on the AFEPL), to identify and keep track of keys.

5.21.3. (Added-AFMC) When not attended or used, keys providing access to SECRET or CONFIDENTIAL information shall be secured in a GSA approved security container, or in a non-GSA approved container constructed of at least 20-guage steel, or material of equivalent strength, and having a built-in GSA approved combination lock or high security key operated padlock.

5.21.4. (Added-AFMC) Keys shall not be removed from the premises, and both keys and locks will be audited monthly. The audit is documented using AF Form 2427, **Lock and key Control Register**.

5.22. Procurement of New Storage Equipment. *[Reference DoD 5200.1-R, Paragraph 6-403]*

5.22.1. Requesters of exceptions send their requests through command ISPM channels to HQ USAF/XOFI. HQ USAF/XOFI will notify OASD(C3I) of the exception. ***[Reference DoD 5200.1-R, Paragraph 6-403a]***

5.22.2. See AFMAN 23-110, Volume II, *Standard Base Supply Customer's Procedures. [Reference DoD 5200.1-R, Paragraph 6-403b]*

5.23. Equipment Designations and Combinations.

5.23.1. See AFMAN 14-304 for guidance on marking security containers used to store SCI. *[Reference DoD 5200.1-R, Paragraph 6-404a]*

5.23.2. Personnel will use SF Form 700, **Security Container Information** (available through the Air Force Publications Distribution system), for each vault or secure room door and security container, to record the location of the door or container, and the names, home addresses, and home telephone numbers of the individuals who are to be contacted if the door or container is found open and unattended. Personnel will affix the form to the vault or secure door or to the inside of the locking drawer of the security container. *[Reference DoD 5200.1-R, Paragraph 6-404b(3)]*

5.23.3. When SF Form 700, Part II, is used to record a safe combination, it must be:

5.23.3.1. Marked with the highest classification level of material stored in the security container; and,

5.23.3.2. Stored in a security container other than the one for which it is being used.

5.24. Repair of Damaged Security Containers. *[Reference DoD 5200.1-R, Paragraph 6-405]*

5.24.1. Locksmiths must either have a favorable National Agency Check or must be continuously escorted while they are repairing security containers. See guidance for unescorted entry to restricted areas in AFI 31-501.

5.24.2. The Naval Facilities Engineering Service Center Technical Data Sheet (TDS) 2000-SHR can be obtained from the Naval Facilities Engineering Services Center (NFESC), 1100 23rd Avenue, Code ESC66, Port Hueneme, California 93043-4370. *[Reference DoD 5200.1-R, Paragraph 6-405b]*

5.24.3. Personnel who have had their GSA approved security containers repaired, must have the locksmith confirm that the container still meets GSA standards. If there is doubt, personnel may contact the DoD Lock Hotline managed by NFESC (DSN 551-1212) or GSA through supply channels for assistance. Personnel must note their findings and the source of confirmation on an AFTO Form 36 and retain that record in the container.

5.25. Maintenance and Operating Inspections. Personnel will follow maintenance procedures for security containers provided in Air Force Technical Order (AFTO) 00-20F-2, *Inspection and Preventive Maintenance Procedures for Security Type Equipment*. *[Reference DoD 5200.1-R, Paragraph 6-406]*

5.25. (AFMC) Any 080 security specialist can perform preventive maintenance inspections on approved GSA security containers as required by TO 00-20F-2, *Inspection and Preventive Maintenance Procedures for Classified Storage Containers*. The inspection is conducted following instructions in paragraph 7 of the TO. Record the inspection on AFTO Form 36, **Maintenance Record For Security Type Equipment**.

5.26. Reproduction of Classified Material.

5.26.1. Unit commanders and staff agency chiefs and Air Staff and Secretariat directors designate equipment for reproducing classified material.

5.26.2. Information managers approve equipment and issue procedures for clearing copier equipment of latent images.

5.26.3. Unit security managers:

5.26.3.1. Post equipment approved for copying classified material;

5.26.3.2. Develop security procedures that ensure control of reproduction of classified material; and,

5.26.3.3. Ensure personnel understand their security responsibilities and follow procedures.

5.27. Control Procedures. Unit commanders and staff agency chiefs designate people/positions to exercise reproduction authority for classified material in their activities. Also see DoD 5200.1-R, paragraph 6-309, and paragraph **5.18.** of this AFI. *[Reference DoD 5200.1-R, Paragraph 6-502]*

Section 5D—Disposition and Destruction of Classified Material

5.28. Retention of Classified Records.

5.28.1. Personnel follow the disposition guidance in AFMAN 37-139. *[Reference DoD 5200.1-R, Paragraph 6-700a]*

5.28.2. Information Security Program Managers will ensure that management of retention of classified material is included in oversight and evaluation of program effectiveness. *[Reference DoD 5200.1-R, Paragraph 6-700b]*

5.28.2. (AFMC) Reductions in classified holdings is a continuing key objective within the Air Force and AFMC aggressive support of that objective is the basis for this requirement. Servicing ISPM program implementing directives will establish such processes as are necessary to ensure an ongoing effort throughout the organizations they service to achieve reductions in classified holdings. These processes will be used by the ISPM during program reviews as a starting point for evaluating management of retention of classified material within the organization. Other considerations might include visible organizational policies regarding the reducing of classified holdings, or changes in type and level of activity within the organization which impact the generation of classified documents or material or the amounts routinely received. The number of shredders available, along with education in their desired use and ease of access may also contribute to reduction of classified holdings.

5.28.3. Unit commanders and staff agency chiefs will designate a “clean-out day” once a year to ensure personnel are not retaining classified material longer than necessary. *[Reference DoD 5200.1-R, Paragraph 6-700b]*

5.28.3. (AFMC) The second Friday of March is the annual clean-out day for AFMC Centers and Staff Agencies. Another date may be chosen if there are compelling local requirements.

5.29. Methods and Standards. *[Reference DoD 5200.1-R, Paragraph 6-701b]*

5.29.1. Personnel may obtain information on GSA specifications for equipment and standards for destruction of other than electronic media and the like from the local supply office.

5.29.1. (AFMC) The installation commander is responsible for ensuring an adequate local destruction capability exists to dispose of classified material. As a means of consolidating local destruction requirements installation commander may establish a central destruction activity to dispose of classified material for agencies supported. Actual destruction of classified material remains the responsibility of the user activity.

5.29.2. Records of Destruction.

5.29.2.1. Top Secret. TSCOs will ensure:

5.29.2.1.1. Two people with Top Secret access are involved in the destruction process;

5.29.2.1.2. Destruction is recorded on one of these forms: AF Form 143; AF Form 310; or, AF Form 1565, **Entry, Receipt, and Destruction Certificate**; and,

5.29.2.1.3. The destruction record is attached to the AF Form 143 (used to account for the document) when the destruction is not recorded on the AF Form 143 itself.

5.29.2.2. Secret and Confidential. A record of destruction is not required but an appropriately cleared person must be involved in the destruction process.

5.29.2.2. (AFMC) When a record must be kept of destroyed Secret or Confidential materials, choose from AF Form 310, AF Form 145 or AF Form 1565.

5.29.2.3. Foreign Government Information. See DoD 5200.1-R, Chapter 6, Section 6, for destruction of foreign government information.

5.29.2.4. Destruction of AIS Media. Dispose of AIS media according to AFSSI 5020, *Remanence Security*.

5.29.2.5. Disposition of Destruction Records. Dispose of destruction records according to AFMAN 37-139.

5.29.2.6. (Added-AFMC) For a listing of National Security Agency (NSA) evaluated and approved destruction devices see Annex B to NTISSI No. 4004. You may request a copy of this document by writing to NSA Media Destruction, Maryland Procurement Office, 9880 Savage Road, Ste 6718, Fort Meade MD 20755-6718.

Section 5E—Alternative or Compensatory Control Measures

5.30. General. *[Reference DoD 5200.1-R, Paragraph 6-800]*

5.30.1. The authority to approve alternative or compensatory security controls is delegated to the ISPM. ISPMs will forward a copy of documentation through command ISPM channels to HQ USAF/XOFI. The documentation must describe the thought process that led up to the decision. *[Reference DoD 5200.1-R, Paragraph 6-800a]*

5.30.1. (AFMC) Paragraph 5.18.1(Added), this supplement, applies.

5.30.1.1. ISPMs may use AF Form 116, **Request for Deviation from Security Criteria** (available on the AFEPL), to document the scenario and approval.

5.30.2. The Air Force doesn't authorize use of security controls listed in DoD 5200.1-R, paragraph 6-800c. *[Reference DoD 5200.1-R, Paragraph 6-800c]*

5.30.3. Send requests to use alternative or compensatory security controls for the safeguarding of NATO or foreign government information through command ISPM channels to HQ USAF/XOFI. *[Reference DoD 5200.1-R, Paragraph 6-800f]*

Chapter 6

TRANSMISSION AND TRANSPORTATION

Section 6A—Methods of Transmission or Transportation

6.1. General Policy.

6.1.1. HQ USAF/XOFI establishes Air Force procedures for transmission and transportation of classified information and material. *[Reference DoD 5200.1-R, Paragraph 7-100a]*

6.1.2. Transmitting Classified Material by Pneumatic Tube Systems. Installation commanders approve the use of pneumatic tube systems and ensure that the equipment and procedures provide adequate security. *[Reference DoD 5200.1-R, Paragraph 7-100a]*

6.1.3. Personnel may get information about transmitting and transporting COMSEC information through their local COMSEC manager. *[Reference DoD 5200.1-R, Paragraph 7-100b]*

6.1.4. Personnel go direct to owners of other agency information to request permission to release the information outside the Department of Defense. *[Reference DoD 5200.1-R, Paragraph 7-100d]*

6.2. Transmitting Top Secret Information. *[Reference DoD 5200.1-R, Paragraph 7-101]*

6.2.1. Electronic Means. Personnel will get information about transmitting Top Secret information via electronic means from their Information Assurance Office. *[Reference DoD 5200.1-R, Paragraph 7-101b]*

6.2.2. DoD Component Courier Service. The Air Force does not have its own courier service. *[Reference DoD 5200.1-R, Paragraph 7-101d]*

6.2.3. Department of State Diplomatic Courier Service. Personnel who need to transport classified material use the Department of State courier system when: *[Reference DoD 5200.1-R, Paragraph 7-101e]*

6.2.3.1. Transmitting any classified material through or within countries hostile to the United States or any foreign country that may inspect it.

6.2.3.2. Transmitting Top Secret material to an installation serviced by diplomatic pouch. Personnel can find out if they are serviced by diplomatic pouch through their local military postal office.

6.3. Transmitting Secret Information. *[Reference DoD 5200.1-R, Paragraph 7-102]*

6.3.1. Also see AFI 31-601. *[Reference DoD 5200.1-R, Paragraph 7-102b]*

6.3.2. The Air Force authorizes the use of the current holder of the General Services Administration contract for overnight delivery of Secret information in urgent cases and when the transmission is between DoD Components within the United States and its Territories. This applies to locations in Alaska, Hawaii, and Guam when overnight delivery is possible. OASD(C3I) has already ensured the conditions cited in DoD 5200.1-R, paragraph 7-102c, have been met. *[Reference DoD 5200.1-R, Paragraph 7-102c]*

6.3.3. For more information on protective security service carriers, see DoD 5220.22-R, *Industrial Security*, AFI 31-601, and AFPD 24-2, *Preparation and Movement of Air Force Material. [Reference DoD 5200.1-R, Paragraph 7-102h]*

6.3.4. Also see guidance in DoD 5200.1-R, paragraph 7-104. *[Reference DoD 5200.1-R, Paragraph 7-102j]*

6.4. Transmitting Confidential Information. *[Reference DoD 5200.1-R, Paragraph 7-103]*

6.4.1. Since first class mail bearing the "Postmaster" notice is an option for transmitting Confidential material, recipients must protect it as Confidential material unless they determine the contents are unclassified. ***EXCEPTION:*** First class mail bearing the notice awaiting distribution at the Base Information Transfer Center (BITC). At this point, such mail will be handled the same as all other First Class Mail.

6.4.1.1. The outer envelope or wrapper shall be endorsed with "Return Service Requested" instead of "POSTMASTER: Do Not Forward."

6.5. Transmission of Classified Material to Foreign Governments. *[Reference DoD 5200.1-R, Paragraph 7-104]*

6.5.1. Also see AFI 31-601 and AFPD 16-2, *Disclosure of Military Information to Foreign Governments and International Organizations. [Reference DoD 5200.1-R, Paragraph 7-104a]*

6.5.2. Personnel may not ship US classified material from a US industrial activity to a foreign entity. *[Reference DoD 5200.1-R, Paragraph 7-104a]*

Section 6B—Preparation of Material for Transmission

6.6. Envelopes or Containers. *[Reference DoD 5200.1-R, Paragraph 7-200]*

6.6.1. Personnel may use AF Form 2595, **Classified Protection Insertion Sheet**, as a countermeasure for the possible threat posed by the chemical composition referred to as "Liquid Window." *[Reference DoD 5200.1-R, Paragraph 7-200a]*

6.6.2. For the purpose of this policy, an activity is a facility. *[Reference DoD 5200.1-R, Paragraph 7-200a(5)]*

6.6.3. Personnel do not use an outer container when entering Secret and below material into the BITC. The pouch is considered the outer container.

6.6.4. Receipts. See receipting requirements at paragraph **5.10.1.1.**

6.6.4.1. Senders trace receipts when they're not acknowledged:

6.6.4.1.1. Within 30 days for material sent within continental United States (CONUS).

6.6.4.1.2. Within 45 days for material sent outside CONUS.

6.6.4.2. The recipient must immediately date, sign, correct, and return the receipt to the sender.

6.6.4.3. If recipients do not return the receipt and confirm they have not received the material, the sending activity must initiate security incident procedures according to **Chapter 9** of this AFI.

Section 6C—Escort or Handcarrying of Classified Material

6.7. General Provisions. *[Reference DoD 5200.1-R, Paragraph 7-300]*

6.7.1. Authorization. *[Reference DoD 5200.1-R, Paragraph 7-300a(3)]*

6.7.1.1. The unit commander, staff agency chief, orders-approving official, security manager, or supervisor authorizes appropriately cleared couriers to handcarry classified material on commercial flights. See DoD 5200.1-R, paragraph 7-301, for required documentation.

6.7.1.2. The unit commander, staff agency chief, orders-approving official, security manager, or supervisor authorizes appropriately cleared couriers to handcarry classified material by means other than on commercial flights.

6.7.1.2. (AFMC) As a minimum, couriers must have verbal authorization to hand-carry classified material outside their normal work areas. This approval alone is sufficient when the courier remains within the confines of an access controlled installation perimeter and does not pass through an entry/exit personnel control point. Personnel hand-carrying outside of work areas must use an envelope, folder, or other closed container to prevent loss or observation of the material. Appropriate cover sheets for classified must also be used.

6.7.1.3. (Added-AFMC) Servicing ISPMs are authorized to approve the overseas hand-carrying of classified information aboard commercial passenger aircraft.

6.7.2. Security managers or supervisors brief each authorized member handcarrying classified material. *[Reference DoD 5200.1-R, Paragraph 7-300b]*

6.7.3. Each Air Force activity or unit that releases classified material to personnel for handcarrying: *[Reference DoD 5200.1-R, Paragraph 7-300b(8)(c)]*

6.7.3.1. Maintains a list of all classified material released.

6.7.3.2. Keeps the list until they confirm all the material reaches the recipient's activity or unit.

6.8. Documentation. Unit commanders, staff agency chiefs, and security managers issue and control DD Form 2501, **Courier Authorization** (available through the Air Force Publications Distribution system), for handcarrying classified material by means other than on commercial flights. This doesn't preclude the use of a courier authorization letter for infrequent courier situation (see paragraph **6.7.1.2.** of this AFI). ***EXCEPTION:*** Documentation is not necessary when handcarrying classified information to activities within an installation (i.e., Air Force installation, separately located missile field). ***NOTE:*** Account for DD Form 2501 as prescribed in AFI 37-161, *Distribution Management.* *[Reference DoD 5200.1-R, Paragraph 7-301]*

6.8. (AFMC) Use DD Form 2501 when handcarrying within the local area and the courier is required to pass through a manned check point or entry point. DD Form 2501 is carried only when handcarrying classified. Otherwise, the completed form is secured within the issuing organization. Use a courier letter when handcarry will be outside the local area. The boundaries of the local area are determined by the servicing ISPM.

6.9. Handcarrying or Escorting Classified Material Aboard Commercial Passenger Aircraft. *[Reference DoD 5200.1-R, Paragraph 7-302a(e)]***.**

6.9.1. The expiration is not to exceed 7 days from the date of issue.

Chapter 7

SPECIAL ACCESS PROGRAMS

7.1. Control and Administration. *[Reference DoD 5200.1-R, Paragraph 8-102c]*

7.1.1. The Office of the Director for Security and Investigative Programs (SAF/AAZ) administers special access programs for the Air Force. See AFPD 16-7, *Special Access Programs.* ***EXCEPTION:*** HQ USAF/XOI controls SCI programs.

7.2. Code Words and Nicknames. Unit commanders, heads of staff agencies, or acquisition system program directors: *[Reference DoD 5200.1-R, Paragraph 8-103d(2)]*

7.2.1. Obtain code words and nicknames through channels from the servicing control point (normally, the MAJCOM, FOA, DRU Information Management activity).

7.2.1.1. (Added-AFMC) HQ AFMC/LGSW assigns nicknames and annually surveys all OPRs of current nicknames to validate, confirm or cancel sponsor information.

7.2.1.2. (Added-AFMC) HQ AFMC staff agencies request a nickname through the HQ AFMC/LGSW web page at *http//www.afmc.wpafb.af.mil/HQ-AFMC/LG/lgs/milgov/project.htm.*

7.2.1.3. (Added-AFMC) Field activities submit unclassified requests, including all necessary information, via e-mail or letter to the HQ AFMC functional OPR. Upon concurrence, the HQ AFMC OPR sends the request to HQ AFMC/LGSW.

7.2.1.4. (Added-AFMC) Upon receipt of nickname assignment, the HQ AFMC OPR notifies all interested activities of nickname assignments and HQ AFMC/LGSW of project completion or termination of nickname need.

7.2.1.5. (Added-AFMC) HQ AFMC/LGSW sends information regarding the nickname assignment and its related meaning to OPRs on a need-to-know basis.

Chapter 8

SECURITY EDUCATION AND TRAINING

Section 8A—Policy

8.1. General Policy. Training is the key to an effective information security program. Commanders at all levels are responsible for ensuring security personnel are adequately trained to perform their duties whether full time or part time. ISPMs are responsible for developing and overseeing all information security program training. *[Reference DoD 5200.1-R, Paragraph 9-100]*

8.1. (AFMC) Commanders and Staff Agency Chiefs must have active training programs. Servicing ISPM policies must include the requirement for organizations to develop and implement a local training plan to ensure effective training of all assigned personnel. The plan must outline the type of training, frequency required, subjects to be presented at each session, and how the training will be accomplished. Use of locally developed software programs for presenting the training via automated information systems is the most desired approach. A sample-training plan is provided at Attachment 3. ISPMs are encouraged to invite OPRs for other security disciplines, such as OPSEC, COMPUSEC and Counter Intelligence (CI), to include their training in the ISPM schedule. This would minimize the training footprint on each serviced organization and show the correlation of these security disciplines.

8.2. Methodology. Commanders and supervisors must ensure that training is properly documented in the individual's official personnel records and ensure personnel receive appropriate credit for attending and completing courses. They must follow the process outlined in AFPD 36-22, *Military Training,* AFI 36-2201, *Developing, Managing, and Conducting Training,* and AFPAM 36-2211, *Guide for Management of Air Force Training System. [Reference DoD 5200.1-R, Paragraph 9-101]*

8.2. (AFMC) All training must be documented IAW applicable DoD/AF directives or as locally determined. This includes the categories of training described in DoD 5200.1-R, Chapter 9, as Initial, Special Requirements, Others and Recurring and Refresher Training. As a minimum, one time training documentation is retained as long as the employee is performing the duties which mandate the training. Recurring training documentation, as a minimum, is retained for the current and preceding calendar year. Documentation methodology must allow tracking of the training to determine date of training, subject areas covered, identity of attendees and percentage of the target group actually receiving/completing the training. Procedures must be in-place to identify, and provide timely make-up for those missing regularly scheduled training.

8.2.1. (Added-AFMC) The goal is to automate all training to the extent that trainees participate from their work locations and at their own pace in order to minimize trainee time away from their work areas. ISPMs are encouraged to pursue local development of computer based training programs and to provide a copy of their successful products to HQ AFMC/SFXP. HQ AFMC/SFXP will serve as a clearing point for these products and cross feed them to all ISPMs.

Section 8B—Initial Orientation

8.3. Cleared Personnel. *[Reference DoD 5200.1-R, Paragraph 9-200]*

8.3.1. Initial Training. Supervisors provide initial training to cleared personnel. *[Reference DoD 5200.1-R, Paragraph 9-200a]*

8.3.2. Also see paragraph **5.4.** of this AFI. *[Reference DoD 5200.1-R, Paragraph 9-200b]*

8.4. Uncleared Personnel. Supervisors provide training to uncleared personnel. *[Reference DoD 5200.1-R, Paragraph 9-201]*

Section 8C—Special Requirements

8.5. Original Classifiers. ISPMs are responsible for administering training to original classifiers. They may either develop their own training or administer the Defense Security Service (DSS) OCA training (formerly a DoDSI training product). *[Reference DoD 5200.1-R, Paragraph 9-301]*

8.6. Declassification Authorities Other Than Original Classifiers. ISPMs will conduct this training. *[Reference DoD 5200.1-R, Paragraph 9-302]*

8.7. Derivative Classifiers, Security Personnel and Others. *[Reference DoD 5200.1-R, Paragraph 9-303]*

8.7.1. Derivative Classifiers. Unit commanders, staff agency chiefs, and supervisors ensure derivative classifiers receive training. ISPMs can assist in finding or developing the appropriate training.

8.7.2. Security Personnel and Others. Unit commanders, staff agency chiefs, and supervisors ensure security career personnel and security managers receive training as follows:

8.7.2.1. Security Career Personnel.

8.7.2.1.1. Civilians. See the Air Force Civilian Security Career Program Master Development Plan. This is a career development guide for security professionals. A copy can be obtained from the MAJCOM, FOA, or DRU civilian security career program coordinator normally located on the ISPM's staff.

8.7.2.1.2. Military. See requirements for award of Special Experience Identifier (SEI) 322 in AFMAN 36-2108, *Airman Classification*. Also use the Air Force Civilian Security Career Program Strategic Action Plan as a guide for determining additional training.

8.7.2.2. Unit or Staff Agency Security Managers. The servicing ISPM can either develop training or have the military or civilian member complete the DSS basic information security orientation course (formerly a DoDSI training course). Supervisors will ensure civilians performing these duties receive the appropriate skill coding in their personnel records according to AFMAN 36-505, *Skill Coding.*

8.7.2.2. (AFMC) Servicing ISPMs conduct initial and refresher Security Manager Training following the subject areas listed in DoD 5200.1-R, paragraph 9-303 and other areas as deemed appropriate. As a minimum, new security managers will receive initial training within 60 days of being assigned as security manager. Persons being re-assigned to security manager duties, after not having performed those duties in the preceding 36 months, should be trained as new security managers. The ISPM conducts Security Manager Meetings periodically throughout the year for purposes of addressing program issues and to inform security managers of new or changing program policies and procedures. ISPMs forward a copy of the meeting minutes to HQ AFMC/SFXP within 30 days following the meeting, and maintain record copies of minutes for the current and previous year.

8.7.2.3. Training Costs. Unit commanders and staff agency chiefs must budget annually for their security program (training courses/aids, awareness products, etc.).

8.8. Others. *[Reference DoD 5200.1-R, Paragraph 9-304]*

8.8.1. ISPMs will identify training requirements in areas that are their responsibility.

8.8.2. For training requirements pertaining to storing, processing, or transmitting classified information in an automated information system, see AFI 33-204, *The C4 Systems Security Awareness, Training, and Education (SATE) Program*. *[Reference DoD 5200.1-R, Paragraph 9-304a]*

8.8.3. For training requirements or briefings pertaining to foreign travel or foreign attendance, see the servicing AFOSI Detachment. *[Reference DoD 5200.1-R, Paragraph 9-304b]*

8.8.4. For training requirements regarding involvement in international programs, see the servicing foreign disclosure office. *[Reference DoD 5200.1-R, Paragraph 9-304e]*

8.8.5. For training requirements regarding acquisition programs subject to the AFI 31-700 series, *Acquisition*, see the servicing acquisition security office. *[Reference DoD 5200.1-R, Paragraph 9-304f]*

Section 8D—Continuing Security Education/Refresher Training

8.9. Recurring and Refresher Training. Unit commanders, staff agency chiefs, and supervisors ensure that each person receives recurring training throughout the duty assignment. Tailor the training to mission needs and design it to address an individual's security responsibilities. This recurring training includes ensuring individuals have the most current security guidance applicable to their responsibilities. Recurring training might include original classification, derivative classification, marking classified documents, safe custodian responsibilities, reporting security incidents, end-of-day security checks, access requirements, etc. *[Reference DoD 5200.1-R, Paragraphs 9-400 and 9-401]*

8.9. (AFMC) Because of the volume of information to be covered, Recurring and Refresher Training should, as a minimum, be presented in semi-annual sessions. Quarterly sessions are recommended for maximum motivational and retentive effect. A sample training plan is presented at Attachment 3.

Section 8E—Termination Briefings

8.10. Procedures. Supervisors or security managers conduct termination briefings by: *[Reference DoD 5200.1-R, Paragraph 9-500]*

8.10.1. Using AF Form 2587, **Security Termination Statement**, to document the briefing.

8.10.2. Debriefing all individuals with security clearance eligibility when they terminate civilian employment, separate from the military service, have their access suspended or terminated, or have their clearance revoked or denied.

8.10.2.1. For NATO access termination briefings, see DoDD 5100.55, United States Security Authority for North Atlantic Treaty Organization Affairs, 21 Apr 82.

8.10.2.2. For SCI access termination briefings, see your servicing special security office.

8.10.2.3. For SIOP-ESI access termination briefings, see AFI 10-1102, *Safeguarding the Single Integrated Operational Plan (SIOP).*

8.10.3. Disposing of AF Form 2587 according to AFMAN 37-139.

8.11. Refusal to Sign a Termination Statement. When an individual willfully refuses to execute AF Form 2587, the supervisor, in the presence of a witness:

8.11.1. Debriefs the individual orally.

8.11.2. Records the fact that the individual refused to execute the termination statement and was orally debriefed.

8.11.3. Ensures the individual no longer has access to classified information.

8.11.4. Forwards it to the servicing ISPM for Security Information File (SIF) processing according to AFI 31-501.

8.11.5. Maintains the SIF according to AFMAN 37-139.

Section 8F—Program Oversight

8.12. General. ISPMs are responsible for ensuring systems are set up to determine training requirements, develop training, and evaluate effectiveness of the training. *[Reference DoD 5200.1-R, Paragraph 9-600]*

8.12. (AFMC) Servicing ISPMs will evaluate training effectiveness in organizations during program reviews.

Chapter 9

POTENTIAL OR ACTUAL COMPROMISE OF CLASSIFIED INFORMATION

9.1. Policy. *[Reference DoD 5200.1-R, Paragraph 10-100]*

9.1.1. A potential compromise is when an investigating official concludes that a compromise probably occurred as a result of the security incident.

9.1.2. Security incidents as used in this AFI pertain to any security violation or infraction as defined in EO 12958.

9.1.3. Report all automated information system (AIS) incidents to the local ISPM and computer security personnel so these officials may evaluate the impact of the incident on national security and the organization's operations. Also see AFI 33-212, *Reporting COMSEC Incidents. [Reference DoD 5200.1-R, Paragraph 10-100b]*

9.1.3. (AFMC) Security incidents involving classified national security information in automated information systems are reported to the servicing ISPM for processing IAW with this supplement.

9.1.4. See AFMAN 14-304. *[Reference DoD 5200.1-R, Paragraph 10-100c]*

9.2. Reporting. *[Reference DoD 5200.1-R, Paragraph 10-101]*

9.2.1. Personnel who learn of a security incident must promptly report it to their servicing ISPM by the end of the first duty day. The ISPM will assign a case number beginning with calendar year, base, and sequential number for tracking purposes. *[Reference DoD 5200.1-R, Paragraph 10-101a]*

9.2.2. Classify notices of incidents at the same level of classification as the information involved in the incident whenever the information is accessible to unauthorized personnel. Such notices must remain classified until the information has been retrieved and appropriately safeguarded. The authority for classifying the notices is the same as for the classified information involved in the compromise. This helps divert attention from the fact that classified information is in a location accessible to unauthorized personnel. *[Reference DoD 5200.1-R, Paragraph 10-101a and c]*

9.2.3. Personnel must report compromises/potential compromises of these incidents through command ISPM channels to HQ USAF/XOFI: *[Reference DoD 5200.1-R, Paragraphs 10-101c—d]*

9.2.3. (Added-AFMC) The servicing ISPM will notify HQ AFMC/SFXP by the end of the next duty day following discovery of these incidents.

9.2.3.1. Classified in the public media;

9.2.3.2. Foreign intelligence agencies;.

9.2.3.3. Criminal activity;

9.2.3.4. NATO classified information;

9.2.3.5. Foreign government information or foreign nationals; and,

9.2.3.6. Restricted Data (RD) or Formerly Restricted Data (FRD).

9.2.4. Personnel must also report these incidents to the servicing AFOSI detachment. They are those involving:

9.2.4.1. Foreign intelligence agencies.

9.2.4.2. Criminal activity.

9.2.5. See paragraph **9.2.3.** *[Reference DoD 5200.1-R, Paragraph 10-101e]*

9.2.6. Personnel report all compromises involving special access information to SAF/AAZ through the appropriate special access program channels. *[Reference DoD 5200.1-R, Paragraph 10-101i]*

9.2.7. (Added-AFMC) The installation ISPM must submit the Security Incident Data Report to HQ AFMC/SFXP NLT 15 Jan and 15 Jul each year via RCS: HAF-SFI(SA)9222. The report will cover security incidents occurring in the preceding six months and will categorize the incidents as follows. Each security incident must also be annotated to show whether it involved a security violation (compromise/possible compromise) or security infraction. A security "infraction" is any incident that is NOT expected to result in an unauthorized disclosure of classified information.

9.2.7.1. (Added-AFMC) Unauthorized Access

9.2.7.2. (Added-AFMC) Mismarking

9.2.7.3. (Added-AFMC) Unauthorized Transmission

9.2.7.4. (Added-AFMC) Improper Storage

9.2.7.5. (Added-AFMC) Unauthorized Reproduction

9.2.7.6. (Added-AFMC) Improper Classification

9.2.7.7. (Added-AFMC) Improper Destruction

9.2.7.8. (Added-AFMC) Other

9.3. Investigation. *[Reference DoD 5200.1-R, Paragraph 10-102a and b]*

9.3.1. The Air Force investigates all security incidents using AFI 90-301, *Inspector General Complaints (Category II Investigations)* and the Inspector General (IG) Investigating Officer's (IO) Guide as guides through the process. Investigating officials can obtain a current copy of the IG IO Guide from their local IG office. Investigations can be as simple as that of a preliminary inquiry or as formal as an investigation with signed sworn statements. The depth of an investigation will be determined by the complexity and seriousness of an incident. The main point of the investigative process is to gain enough information to determine if a compromise has occurred so that the appropriate corrective action can be taken.

9.3.1. (Added-AFMC) To determine the circumstances of occurrence, a preliminary inquiry is immediately initiated into incidents of compromise, possible compromise, or an infraction of the safeguarding controls established by Executive Order 12958 and/or DoD and Air Force implementing directives. A formal investigation is conducted into complex incidents or those of serious consequence. The servicing ISPM oversees processing of incidents involving collateral classified information, while incidents involving SCI or SAP classified information are handled through those program channels. In addition to the requirements in DoD 5200.1-R, para 10-102, the inquiry or investigation determines:

9.3.1.1. (Added-AFMC) Whether or not a security incident has occurred.

9.3.1.2. (Added-AFMC) Appropriate measures or actions to minimize or negate the adverse effect of the security incident.

9.3.1.3. (Added-AFMC) The seriousness of damage to United States interests.

9.3.1.4. (Added-AFMC) Appropriate remedial (or corrective) action to prevent the reoccurrence of similar incidents.

9.3.2. Appointing Investigative Officials.

9.3.2.1. Unit commanders or staff agency chiefs of the activity responsible for the security incident appoint an investigative official, as appropriate, to conduct an investigation according to this instruction. They may use the sample appointment letter in their local IG IO Guide as their appointment letter format.

9.3.2.1. (AFMC) The unit commander, director or staff agency chief appoints the preliminary inquiry official by the end of the first duty day following discovery. The preliminary inquiry official forwards the preliminary inquiry report to the appointing official within 10 workdays from appointment. The appointing official may grant extensions when fully justified.

9.3.2.2. When security incidents occur because of unauthorized transmission of classified material, the sending activity's unit commander or staff agency chief appoints the investigative official.

9.3.2.3. Investigative officials coordinate their actions with the servicing ISPM and staff judge advocate's office.

9.3.2.3. (AFMC) Coordinate with the Staff Judge Advocate's office to ensure the inquiry is conducted IAW legal requirements. This is particularly important as it relates to interviewing, administering of oaths and the process followed in evaluating information to reach a determination of responsibility for the incident. When these considerations are not present, and the inquiry official is fully experienced in conducting investigations the JAG coordination is optional.

9.3.3. (Added-AFMC) Preliminary Inquiry.

9.3.3.1. (Added-AFMC) The servicing ISPM forwards a copy of closed preliminary inquiry reports involving compromise or possible compromise to HQ AFMC/SFXP. Forward these reports within 10 workdays of closure.

9.3.3.2. (Added-AFMC) A preliminary inquiry establishes that a security infraction or loss or compromise of classified information did not occur; or

9.3.3.3. (Added-AFMC) That a security infraction occurred constituting a knowing, willful or negligent action contrary to Information Security Program implementing directives, but not involving the loss or compromise of classified information.

9.3.3.4. (Added-AFMC) That a loss or compromise of classified information did occur but the compromise reasonably could not be expected to cause damage to the national security. If in such instances the official finds no indication of significant security weakness, the report of preliminary inquiry will be sufficient to resolve the incident; or

9.3.3.5. (Added-AFMC) That the loss or compromise of classified information did occur and that the compromise reasonably could be expected to cause damage to the national security or that the probability of damage to the national security cannot be discounted.

9.3.3.6. (Added-AFMC) The appointing authority or other designated official notifies the appropriate OCA when there is a loss or compromise of classified information, to include information made public by the news media. Do not delay this notification pending completion of the inquiry once loss or compromise/potential compromise is confirmed. Notifications revealing that classified information is in the public media is classified at the level of the classified information involved.

9.3.3.7. (Added-AFMC) When the preliminary inquiry concludes that a security incident has occurred, the report will include a statement categorizing the incident as either a compromise, possible compromise or security infraction (deviation).

9.3.3.8. (Added-AFMC) An inquiry is not extensive in scope; it gathers available facts to support conclusions or recommendations made by the inquiry official. Upon receipt of the written inquiry report, the appointing authority closes most Air Force information security incidents without opening a formal investigation. This action is based on a determination that no additional substantive information will be obtained by conducting a formal investigation.

9.3.3.9. (Added-AFMC) When the incident circumstances provide a reasonable expectation of damage to national security, close the inquiry and open a formal investigation.

9.3.4. (Added-AFMC) Investigations

9.3.4.1. (Added-AFMC) The unit commander or staff agency chief appoints an investigation official and initiates a formal investigation immediately upon completion of the preliminary inquiry, if warranted by the preliminary inquiry results.

9.3.4.2. (Added-AFMC) A formal investigation is a detailed and thorough examination of evidence to determine the extent and seriousness of the compromise and to fix responsibility for any disregard (deliberate or inadvertent) of governing directives which led to the security incident.

9.3.4.3. (Added-AFMC) Investigations include identification of the source, date and circumstances of the compromise; complete description and classification of each item of classified information compromised; a thorough search for the classified information; identification of any person or procedure responsible for the compromise; an analysis and statement of the known or probable damage to the national security that has resulted or may result, and the cause of the loss or compromise; or a statement that compromise did not occur or that there is minimal risk of damage to the national security.

9.3.4.4. (Added-AFMC) The servicing ISPM monitors and coordinates on reports of investigation.

9.3.4.5. (Added-AFMC) If not previously accomplished during the preliminary inquiry phase, the appointing authority or other designated official notifies the appropriate OCA when there is a loss or compromise of classified information, to include information made public by the news media. Do not delay this notification pending completion of the investigation once loss or compromise/potential compromise is confirmed. Notifications revealing that classified information is in the public media is classified at the level of the classified information involved.

9.4. Results of the Investigation. *[Reference DoD 5200.1-R, Paragraph 10-103]*

9.4.1. Upon completion of the investigation, the appointing official:

9.4.1.1. Closes the investigation unless MAJCOM, DRU, or FOA directives indicate otherwise;

9.4.1.1. (AFMC) Center Commanders close formal investigations of information security program incidents. This includes security incidents involving classified national security information contained in or processed through automated information systems.

9.4.1.2. Determines if administrative or disciplinary action is appropriate. See AFI 31-501 for information on SIFs;

9.4.1.3. Debriefs individuals who have had unauthorized access. Use AF Form 2587. Also see DoD 5200.1-R, paragraph 10-105;

9.4.1.4. Forwards a copy of the report to the ISPM identifying corrective actions taken. The ISPM will use it to help identify specific areas of the security program for enhancement. And,

9.4.1.5. Disposes of the report according to the instructions in AFMAN 37-139.

9.5. Verification, Reevaluation and Damage Assessment. *[Reference DoD 5200.1-R, Paragraph 10-104]*

9.5.1. OCAs:

9.5.1.1. Set up damage assessment controls and procedures for their information;

9.5.1.2. Must notify HQ USAF/XOFI through command ISPM channels when doing a damage assessment; and,

9.5.1.3. Must provide a copy of the damage assessment report to HQ USAF/XOFI through command ISPM channels.

9.5.2. (Added-AFMC) Damage Assessments.

9.5.2.1. (Added-AFMC) The OCA, upon learning that a compromise or possible compromise of specific classified information has occurred, and is reasonably expected to cause damage to national security, shall prepare a written damage assessment. While no time limits are placed on completion of the damage assessment, it must be initiated by the OCA upon notification and completed without undue delay. The OCA must determine whether the damage assessment itself is classified and mark and process accordingly.

9.5.2.2. (Added-AFMC) As a minimum, damage assessments contain the identification of the source, date and circumstances of the compromise; classification of the specific information lost or compromised; a description of the specific information lost or compromised; an analysis and statement of the known or probable damage to the national security; an assessment of the possible advantages to foreign powers; an assessment of the original classification decision regarding the information involved; and an assessment of whether countermeasures are appropriate and feasible to negate or minimize the effect of the compromise.

9.5.2.3. (Added-AFMC) The OCA notifies all known holders of the information involved if classification levels are changed or the information is declassified.

9.5.2.4. (Added-AFMC) OCAs must maintain records of damage assessments they prepare in a manner that facilitates their retrieval and use. Dispose of the records IAW records management directives (AFMAN 37-139). OCAs provide a copy of damage assessments to the servicing ISPM for attachment to the file copy of the security incident.

9.6. Management and Oversight. *[Reference DoD 5200.1-R, Paragraph 10-106]*

9.6.1. The ISPM:

9.6.1.1. Provides technical guidance.

9.6.1.2. Monitors the status of security incidents.

9.6.1.3. Forwards, through command ISPM channels, those incidents involving cases described in paragraph **9.2.3.** above to HQ USAF/XOFI.

9.6.2. Investigative officials must complete investigations within 30 duty days from appointment. They can use the same investigation report format in AFI 90-301 for their report.

9.6.3. HQ USAF/XOFI uses security incident data in their management information system to assist in measuring the health of the program. See paragraph **1.5.** of this AFI and AFPD 31-4.

9.7. Unauthorized Absences. Report unauthorized absences as described in DoD 5200.1-R, paragraph 10-108, to the ISPM and AFOSI detachment. *[Reference DoD 5200.1-R, Paragraph 10-108]*

MARVIN R. ESMOND, Lt Gen, USAF
DCS/Air & Space Operations

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

Executive Order 12958, *Classified National Security Information,* 20 Apr 95

Federal Register Part VI, OMB, 32 CFR Part 2001, ISOO, *Classified National Security Information, Final Rule,* 13 Oct 96

OMB ISOO Directive Number 1, *Classified National Security Information,* 13 Oct 95

DoD 4000.25-8-M, *Military Assistance Program Address Directory System,* Jul 95

DoDD 5100.55, *United States Security Authority for North Atlantic Treaty Organization Affairs,* 21 Apr 82

DoD 5200.1-R, *Information Security Program,* 17 Jan 97

DoD 5200.1-PH, *DoD Guide to Marking Classified Documents,* Apr 97

DoD 5200.1-PH-1, *Classified Information Nondisclosure Agreement (Standard Form 312),* Mar 89

DoDD 5210.2, *Access to and Dissemination of Restricted Data,* Jan 78

DoDD 5210.83, *Unclassified Controlled Nuclear Information (UCNI),* 15 Nov 91

DoD 5220.22-M, *National Industrial Security Program Operating Manual,* Jan 95

DoD 5220.22-R, *Industrial Security Regulation,* Dec 85

DoDI 5240.11, *Damage Assessments,* 23 Dec 91

Naval Facilities Engineering Service Center Technical Data Sheet, TDS-2000-SHR, *Neutralizing "Locked-Out" Security Containers,* Nov 93

RCS Report HAF-SFI(Q)9222, *The Information Security Measurement Report and The Air Force Automatic Declassification Review Summary*

AFI 14-302, *Control, Protection, and Dissemination of Sensitive Compartmented Information*

AFMAN 14-304, *The Security, Use, and Dissemination of Sensitive Compartmented Information (Supersedes USAFINTEL 201-1)*

AFPD 16-2, *Disclosure of Military Information to Foreign Governments and International Organizations*

AFI 16-201, *Foreign Disclosure of Classified and Unclassified Military Information to Foreign Governments and International Organizations*

AFPD 16-7, *Special Access Programs*

AFI 16-701, *Special Access Programs*

AFMAN 23-110, Volume II, *Standard Base Supply Customer's Procedures*

AFPD 24-2, *Preparation and Movement of Air Force Material*

AFI 31-101, Volume I, *Air Force Physical Security Program*

AFI 31-207, *Arming and Use of Force by Air Force Personnel*

AFI 31-700 Series, *Acquisition*

AFPD 31-4, *Information Security*

AFI 31-205, *Air Force Security and Policy Review Program,*

AFI 31-501, *Personnel Security Program Management*

AFI 31-601, *Industrial Security Program Management*

AFPD 33-2, *Information Protection*

AFI 33-202, *Computer Security*

AFI 33-204, *The C4 Systems Awareness, Training, and Education (SATE) Program*

AFI 33-208, *Information Assurance Operations*

AFI 33-211, *Communications Security (COMSEC) User Requirements*

AFI 33-212, *Reporting COMSEC Incidents*

AFI 35-205, *Air Force Security and Policy Review Program*

AFI 36-1001, *Managing the Civilian Performance Program*

AFPD 36-22, *Military Training*

AFMAN 36-2108, *Airman Classification*

AFI 36-2201, *Developing, Managing, and Conducting Training*

AFPAM 36-2211, *Guide for Management of Air Force Training System*

AFI 36-2402, *Officer Evaluation System*

AFI 36-2403, *The Enlisted Evaluation System (EES)*

AFMAN 36-505, *Skill Coding*

AFI 37-131, *Air Force Freedom of Information Act Program*

AFMAN 37-139, *Records Disposition Schedule*

AFI 37-161, *Distribution Management*

AFI 51-301, *Civil Litigation*

AFI 61-204, *Disseminating Scientific and Technical Information*

AFI 61-205, *Sponsoring or Cosponsoring, Conducting, and Presenting DoD Related Scientific Technical Papers at Unclassified and Classified Conferences, Symposia, and Other Similar Meetings*

AFI 65-401, *Relations with the General Accounting Office*

AFI 71-101, Volume I, *Criminal Investigations, Counterintelligence, and Protective Service Matters*

AFI 90-301, *Inspector General Complaints (Category II Investigations)*

AFI 90-401, *Air Force Relations with Congress*

AFTO 00-20F-2, *Inspection and Preventive Maintenance Procedures for Security Type Equipment*

AFSSI 5020, *Remanence Security*

Abbreviations and Acronyms

ADP—Automatic Data Processing

AF—Air Force

AFDO—Air Force Declassification Office

AFI—Air Force Instruction

AFMAN—Air Force Manual

AFOSI—Air Force Office of Special Investigations

AFPD—Air Force Policy Directive

AFPDL—Air Force Publishing Distribution Library

AFSSI—Air Force Special Security Instruction

AFTO—Air Force Technical Order

AIS—Automated Information System

ASCAS—Automated Security Clearance Approval System

BITC—Base Information Transfer Center

CNWDI—Critical Nuclear Weapon Design Information

COMSEC—Communications Security

CONUS—Continental United States

DCII—Defense Clearance and Investigations Index

DCS—Defense Courier Service

DD—Department of Defense (Used for DoD Forms)

DEA—Drug Enforcement Agency

DoD—Department of Defense

DoDD—Department of Defense Directive

DoDI—Department of Defense Instruction

DoDSI—Department of Defense Security Institute

DoE—Department of Energy

DRU—Direct Reporting Unit

DSS—Defense Security Service (Formerly DIS and DoDSI)

DTIC—Defense Technical Information Center

EES—Enlisted Evaluation System

EO—Executive Order

FMS—Foreign Military Sales

FOA—Field Operating Agency

FOIA—Freedom of Information Act

FOUO—For Official Use Only

FRD—Formerly Restricted Data

GAO—General Accounting Office

GILS—Government Information Locator System

GPO—Government Printing Office

GSA—General Services Administration

IDS—Intrusion Detection System

IG—Inspector General

IO—Investigating Officer

ISPM—Information Security Program Manager

ISOO—Information Security Oversight Office

LFC—Local Files Check

MAJCOM—Major Command

MDR—Mandatory Declassification Review

MIS—Management Information System

NAC—National Agency Check

NARA—National Archives and Records Administration

NATO—North Atlantic Treaty Organization

NCR—National Capital Region

NdA—Nondisclosure Agreement

OCA—Original Classification Authority

OMB—Office of Management and Budget

PA—Privacy Act

PCS—Permanent Change of Station

RCS—Report Control Symbol

RD—Restricted Data

SAP—Special Access Program

SATE—Security Awareness, Training, and Education

SCI—Sensitive Compartmented Information

SCG—Security Classification Guide

SEI—Special Experience Identifier

SF—Standard Form

SIF—Security Information File

SSO—Special Security Office

TDS—Technical Data Sheet

TDY—Temporary Duty

TSCA—Top Secret Control Account

TSCM—Technical Surveillance Countermeasures

TSCO—Top Secret Control Officer

UCNI—Unclassified Controlled Nuclear Information

Attachment 2

LIST OF AIR FORCE OFFICIALS AUTHORIZED TO CERTIFY ACCESS TO RESTRICTED DATA

Secretariat

Secretary of the Air Force (SAF/OS)
Under Secretary of the Air Force (SAF/US)
Assistant Secretary of the Air Force (Space) (SAF/SN)
Assistant Secretary of the Air Force (Financial Management and Comptroller) (SAF/FM)
Assistant Secretary of the Air Force (Manpower, Reserve Affairs, Installations, and Environment) (SAF/MI)
Assistant Secretary of the Air Force (Acquisition) (SAF/AQ)
General Counsel (SAF/GC)
Inspector General (SAF/IG)
Administrative Assistant to the Secretary of the Air Force (SAF/AA)

Air Staff

Chief of Staff (HQ USAF/CC)
Vice Chief of Staff (HQ USAF/CV)
Assistant Vice Chief of Staff (HQ USAF/CVA)
Deputy Chief of Staff/Air and Space Operations (HQ USAF/XO)
Director, Intelligence, Surveillance and Reconnaissance (HQ USAF/XOI)
Deputy Chief of Staff/Installations and Logistics (HQ USAF/IL)
Deputy Chief of Staff/Personnel (HQ USAF/DP)
Deputy Chief of Staff/Plans and Programs (HQ USAF/XP)
Surgeon General (HQ USAF/SG)
Director of Security Forces (HQ USAF/XOF)
Chief, Information Security Division (HQ USAF/XOFI)
Chief of Safety (HQ USAF/SE)

Commands

Commander, Air Education and Training Command (HQ AETC/CC)
Commander, Air Force Institute of Technology (HQ AFIT/CC)
Commander, Air University (HQ AU/CC)
Commander, Air Force Space Command (HQ AFSPC/CC)
Commander, 45th Space Wing (HQ 45 SW/CC)
Commander, Air Force Materiel Command (HQ AFMC/CC)
Commander, Ogden Air Logistics Center (OO-ALC/CC)
Commander, Oklahoma City Logistics Center (OC-ALC/CC)
Commander, Sacramento Air Logistics Center (SM-ALC/CC)
Commander, San Antonio Air Logistics Center (SA-ALC/CC)
Commander, Warner Robins Air Logistics Center (WR-ALC/CC)
Commander, Aeronautical Systems Center (HQ ASC/CC)
Commander, Human Systems Center (HQ HSC/CC)
Commander, Air Force Flight Test Center (HQ AFFTC/CC)
Commander, Air Force Development Test Center (HQ AFDTC/CC)
Commander, Arnold Engineering Development Center (HQ AEDC/CC)
Commander, Air Force Research Laboratory (HQ AFRL/CC)
Commander, Electronic Systems Center (HQ ESC/CC)
Commander, Space and Missile Systems Center (HQ SMC/CC)
Commander, Air Force Reserve Command (HQ AFRC/CC)
Commander, Air Mobility Command (HQ AMC/CC)
Commander, Pacific Air Forces (HQ PACAF/CC)
Commander, United States Air Forces in Europe (HQ USAFE/CC)
Commander, Air Combat Command (HQ ACC/CC)

Direct Reporting Units

Commander, 11 Wing (HQ 11 WG/CC)
Commander, United States Air Force Academy (HQ USAFA/CC)
Commander, Air Force Operational Test and Evaluation Center (HQ AFOTEC/CC)
Commander, Air Force Communications Agency (HQ AFCA/CC)

Field Operating Agencies

Commander, Air Intelligence Agency (HQ AIA/CC)
Commander, National Air Intelligence Center (HQ NAIC/CC)

Miscellaneous

Commander, Air Force Technical Applications Center (HQ AFTAC/CC)

Attachment 3

CONTROLLED UNCLASSIFIED INFORMATION

A3.1. For Official Use Only (FOUO). See AFI 37-131, for additional Air Force policy on FOUO information. *[Reference DoD 5200.1-R, Paragraph 2-204]*

A3.2. Sensitive But Unclassified and Limited Official Use Information. Users apply the same marking, accessing, and protecting policy as required for FOUO information, AFI 37-131. *[Reference DoD 5200.1-R, Paragraph 3-300]*

A3.3. Protection of Drug Enforcement Agency (DEA) Sensitive Information. *[Reference DoD 5200.1-R, Paragraph 4-403a]*

A3.3.1. Users follow DEA policy for safeguarding DEA sensitive information.

A3.3.2. See AFI 33-202, *Computer Security*, for policy on secure communications circuits.

A3.4. Unclassified Controlled Nuclear Information (UCNI)

A3.4.1. Responsibility. The Director of Security Forces (HQ USAF/XOF) has primary responsibility within the Air Force for the implementation of DoDD 5210.83. *[Reference DoD 5200.1-R, Appendix C, Section 5]*

A3.4.2. UCNI Officials.

A3.4.2.1. The following positions have been designated UCNI Officials within the Air Force:

A3.4.2.1.1. Air Staff and Secretariat staff agency chiefs.

A3.4.2.1.2. Major command, field operating agency, and direct reporting unit commanders.

A3.4.2.1.3. Installation commanders and equivalent commander positions.

A3.4.2.1.4. Chiefs of Security Forces at all levels.

A3.4.3. UCNI Officials' Responsibilities.

A3.4.3.1. Identify information meeting definition of UCNI.

A3.4.3.2. Determine criteria for access to UCNI and approve special access requests.

A3.4.3.3. Approve or deny the release of UCNI information.

A3.4.3.4. Ensure all UCNI information is properly marked, safeguarded, transmitted, and destroyed properly.

A3.4.3.5. Document decisions and report them through their command ISPM channels to HQ USAF/XOFI. RCS Number DD-C3I(AR)1810 applies to this data collection.

A3.5. Sensitive Information (Computer Security Act of 1987). See AFI 33-202 for Air Force policy on protecting information in Federal Government AIS. *[Reference DoD 5200.1-R, Paragraph 6-600]*

A3.6. Technical Documents. See AFI 61-204 for Air Force policy on technical documents. *[Reference DoD 5200.1-R, Paragraph 7-700]*

Attachment 3 (Added-AFMC)

A3.4.4. (Added-AFMC) Physical Protection Requirements.

A3.4.4.1. (Added-AFMC) When not in use, UCNI shall be stored in a manner affording reasonable and adequate protection against unauthorized access. An unlocked container is adequate inside a controlled or guarded area. In other areas, UCNI shall be stored in a locked drawer, desk, repository, or in a locked room.

A3.4.4.2. (Added-AFMC) UCNI may be reproduced without permission from the originator ONLY to the minimum extent necessary to carry out official duties, and all copies must be marked and protected as the original.

A3.4.4.3. (Added-AFMC) UCNI shall be disposed of by any approved method of destruction for classified matter, or any other method preventing retrieval.

A3.4.4.4. (Added-AFMC) UCNI shall be packaged to prevent disclosure of its presence when transmitted by a means that could allow unauthorized access. It will be transmitted by: U.S. First Class, Express, Certified, or registered mail; any means approved for classified; or handcarry by an authorized person maintaining continuous control.

A3.4.4.5 (Added-AFMC) UCNI may be discussed or transmitted over an unprotected telephone/telecommunications media when required by operational necessity. A more secure means should be used if possible.

Attachment 4

DEPARTMENT OF THE AIR FORCE EXECUTIVE ORDER (EO) 12958 25-YEAR AUTOMATIC DECLASSIFICATION PLAN

Section A4A—Plan

A4.1. Purpose. This plan provides the framework for Air Force compliance with Section 3.4 of the EO 12958.

A4.2. Scope. This plan pertains to all classified Air Force records determined under Federal law to have permanent historical value wherever they may be stored. Examples of record locations or storage are: National Archives (including regional archive branches), Federal Records Centers, Presidential Libraries, unit file rooms or repositories, other approved repositories, including contractor facilities, libraries, and within other agencies.

A4.3. Senior Official. Air Force Senior Security Official: Mr. William A. DAVIDSON, Administrative Assistant to the Secretary of the Air Force. Address - SAF/AA 1720 Air Force, Pentagon, Washington, DC 20330-1720. Telephone - (703) 695-9492.

A4.4. Estimated Amount Of Records And Locations

A4.4.1. The total estimated amount of Air Force records which meet the criteria of Section 3.4 is: 70,598 Cubic Feet (176,495,000 Pages). Of the total figure, 70,288 Cubic Feet (175,720,000 Pages) contain potentially exemptible information. Specific record reviews over the next five (5) years will determine more precisely what records must remain classified and what records can be automatically declassified. The remaining 310 Cubic Feet (775,000 Pages) can be automatically declassified without further review.

A4.4.2. Record locations and the estimated amount for these locations are as follows:

A4.4.2.1. 52,864 Cubic Feet (132,160,000 Pages)—Air Force Command/Activity Files, Repositories, Libraries, and Historical Centers.

A4.4.2.2. 9,644 Cubic Feet (24,110,000 Pages)—Federal Records Centers.

A4.4.2.3. 6,196 Cubic Feet (15,490,000 Pages)—National Archives.

A4.4.2.4. 1,584 Cubic Feet (3,960,000 Pages)—Presidential Libraries.

A4.4.2.5. 310 Cubic Feet(775,000 Pages)—Air Force Command/Activity Files, Repositories, Libraries, and Historical Centers - pages to be automatically declassified without review.

NOTE:

Specific location(s) of Air Force command/activity files is contained in our supporting data and can be provided upon request.

A4.4.3. The survey method used by the Air Force to obtain these figures consisted of tasking each Air Force Secretariat, Air Staff, Major Command, Direct Reporting Unit, and Field Operating Agency activity to search their file holdings to identify records, documents, and information that falls within the purview of EO 12958, Section 3.4. The estimation conversion table provided by ISOO was used.

A4.5. Exempt File Series Description

A4.5.1. Federal Records Center: Record Groups 340, 341, and 342. Reasons for exemption correspond with EO exemption categories 1, 2, 5, 6 and the fact that the files contain some Restricted Data and Formerly Restricted Data.

A4.5.2. National Archives: Category 1 and 3. Reasons for exemption correspond with EO exemption categories 1, 2, 5, and 6.

A4.5.3. Presidential Libraries: Presidential Files. Reasons for exemption correspond with EO exemption categories 1, 2, 5, and 6.

A4.5.4. Air Force Commands/Activities: Various files series are listed as:

A4.5.4.1. Airborne Warning and Control Systems.

A4.5.4.2. Agreements.

A4.5.4.3. Ballistic Missile Systems.

A4.5.4.4. Combat Evaluations.

A4.5.4.5. Command Files.

A4.5.4.6. COMSEC Surveillance Project.

A4.5.4.7. Country Files.

A4.5.4.8. Cryptographic Information.

A4.5.4.9. Cryptologic Information.

A4.5.4.10. Electronic Warfare.

A4.5.4.11. Espionage/Counterespionage Operations.

A4.5.4.12. Flight Technical Reports.

A4.5.4.13. Foreign Civil Litigation Cases.

A4.5.4.14. Foreign Government Agreements.

A4.5.4.15. Foreign Government Technology.

A4.5.4.16. Historical Program and Unit Records.

A4.5.4.17. Intelligence Billet Validation.

A4.5.4.18. Intelligence Material Records.

A4.5.4.19. Intelligence Presentation Aids.

A4.5.4.20. Intelligence Reference Records.

A4.5.4.21. Investigative Files.

A4.5.4.22. Law of Armed Conflict.

A4.5.4.23. Missile/Space Technology.

A4.5.4.24. Munitions Effectiveness/Target Vulnerability.

A4.5.4.25. Negotiating Records.

A4.5.4.26. Nuclear Weapons Information.

A4.5.4.27. Presidential Aircraft System Security Standards.

A4.5.4.28. Security Classification Guides.

A4.5.4.29. Studies, Analysis and Summaries.

A4.5.4.30. Test Plans.

A4.5.4.31. Training Records/Film.

A4.5.4.32. Vietnam.

A4.5.4.33. Weapons Systems.

A4.5.4.34. War Plans.

NOTE:

Reasons for exemption correspond with EO exemption categories 1, 2, 3, 4, 5, 6, 7, 8, 9, and Restricted Data and Formerly Restricted Data.

A4.6. Implementation Plan. The following actions will be taken to ensure the Air Force is in compliance with Section 3.4 of the EO.

A4.6.1. All Air Force activities - Secretariat, Air Staff, Major Commands, Direct Reporting Units, and Field Operating Agencies, that classify and/or maintain classified holdings will be responsible for:

A4.6.1.1. Identifying records, files, documents, and information which falls under the purview of Section 3.4.

A4.6.1.2. Providing specific resources, such as manpower and financial support, that will be allocated to identify records and perform declassification reviews.

A4.6.1.3. Implementing self paced classification/declassification management training.

A4.6.1.4. Conducting declassification reviews on all records which fall within the purview of Section 3.4 and reporting results of their reviews quarterly to HQ USAF/XOFI.

A4.6.1.5. Declassifying, where possible, and making available to the public all records not requiring exemption.

A4.6.2. Declassification reviews and actions will be accomplished by:

A4.6.2.1. Using in place and mobile declassification review teams that are composed of local subject matter experts, security personnel, records management personnel, historians, and reserve personnel.

A4.6.2.2. Conducting bulk declassification with concentration directed first to the high risk records, medium risk second, and low risk last. The following risk definitions apply:

A4.6.2.2.1. High - most of the information contained in the records will almost invariably fall into one or more exemption categories and have information which belongs to other agencies. Therefore, these records will require extensive interagency coordination and review.

A4.6.2.2.2. Medium - some of the information contained in the records will fall into one or more exemption categories and have some information which belongs to another agency. These records may require interagency coordination and review.

A4.6.2.2.3. Low - very little, if any, of the information contained in the records will fall into an exemption category or belong to another agency. These records most likely will require no interagency coordination.

A4.6.2.3. Automating applicable Security Classification and Declassification Guides and making them available to other federal agencies.

A4.6.3. Review goal will be:

A4.6.3.1. 20% of records—15 Nov 95 - 15 Oct 96.

A4.6.3.2. 20% of records—16 Oct 96 - 15 Oct 97.

A4.6.3.3. 20% of records—16 Oct 97 - 15 Oct 98.

A4.6.3.4. 20% of records—16 Oct 98 - 15 Oct 99.

A4.6.3.5. 20% of records—16 Oct 99 - 16 Apr 00.

A4.6.4. Results of automatic declassification review will be monitored through the metric - Air Force Automatic Declassification Review Summary. See AFPD 31-4 for a sample of this metric.

A4.6.5. Air Force will alter its review cycle of security classification guides to correspond with the implementation date of the new order.

A4.6.5.1. Review of all Air Force security classification guides will begin 16 October 1995 with a goal of completing the initial review by October 1997.

A4.6.5.2. The purpose of these reviews will be to update the guides as required and to bring them into alignment with the provisions of the new order.

A4.6.5.3. Declassification guidance will be included in each guide as deemed appropriate.

A4.6.5.4. Classification and declassification guides will be placed in the automated Air Force Declassification Toolbook and will be made available through the Air Force Publishing Distribution Library (AFPDL). Ultimately, all classification and declassification instructions will be placed in a key word searchable automated database that will be made available to all Air Force classifiers.

A4.7. Air Force Database. An Air Force locator system will be developed for use within the Government Information Locator System (GILS). As records are declassified, they will be listed in GILS and made available for public information.

Section A4B—Referrals

A4.8. Purpose. This section establishes the process for handling all information which is subject to the provisions of EO 12958, *Classified National Security Information*, Section 3.4, Automatic Declassification, and has been referred to, within, or outside the Air Force for review.

A4.9. Scope. This process applies to all information requiring review as prescribed by Section 3.4 of EO 12958, and:

A4.9.1. Is clearly Air Force information but is held by an organization outside of the Air Force.

A4.9.2. Is Air Force information being held by one Air Force organization but belongs to another Air Force organization.

A4.9.3. Is information being held by the Air Force but belongs to another organization outside of the Air Force.

A4.10. Primary Points Of Contact.

A4.10.1. Referrals to the Air Force: AFDO, Crystal Plaza 6, 2221 South Clark Street, Suite 600, Arlington, VA, 22202; Telephone numbers - (703) 604-4700 (DSN 664); Fax - (703) 604-5533 (DSN 664).

A4.10.2. Referrals from or within the Air Force: Air Force organization initiating the referral.

A4.10.3. Superseded or disestablished Air Force organization: The Air Force organization that has assumed, either directly or indirectly, the responsibility for the functions of the organization no longer in existence.

A4.11. Referral Process.

A4.11.1. Information forwarded to the Air Force by another government organization will be processed as follows:

A4.11.1.1. AFDO is the central point within the Air Force to receive all information referred to the Air Force for review by another government organization.

A4.11.1.2. AFDO, in turn, will be responsible for receiving all referred information; storing and protecting the information; reviewing the information for classification/declassification determination; forwarding to the appropriate Air Force organization(s) to review for classification/declassification determination as necessary; and responding to the government agency that referred the information, if appropriate.

A4.11.2. Air Force organizations will review their information before a decision is made to refer information from or within the Air Force. An Air Force organization will not refer information to another Air Force organization or to another government organization if it intends to exempt, in full, its own information. Nor will an Air Force organization refer information to another Air Force organization if it can first declassify the information from instructions received in an appropriate Air Force classification/declassification guide. For information that will be referred:

A4.11.2.1. Referrals within the Air Force: If information contained in documents held by one Air Force organization but originated by another Air Force organization is referred to the originating Air Force organization for review, the following applies:

A4.11.2.1.1. Unless agreed to on a case by case basis, only information belonging to the originating organization, plus adequate identifying documentation, will be referred.

A4.11.2.1.2. Method of referral, e.g., paper copy, electronic, CD-ROM, will be based on the capability of the receiving organization.

A4.11.2.1.3. Unless agreed to on a case by case basis, no suspense will be levied by the referring organization.

A4.11.2.2. Referrals to another government organization: If information contained in documents held by an Air Force organization but originated by another government organization is referred to the originating government organization for review, the following applies:

A4.11.2.2.1. Unless agreed to on a case by case basis, only information belonging to the originating organization, plus adequate identifying documentation, will be referred.

A4.11.2.2.2. Method of referral, e.g., paper copy, electronic, CD-ROM, will be based on the capability of the receiving organization.

A4.11.2.2.3. Unless agreed to on a case by case basis, no suspense will be levied by the referring organization.

Attachment 4 (Added-AFMC)

A4.6.4. (AFMC) Serving ISPMs must report the following information concerning local automatic declassification review actions as required by EO 12958, Section 3.4. This information must reach HQ AFMC/SP by the 15th day following the last day of the fiscal quarter (RCS: HAF-SFI(SA)9222 applies):

A4.6.4.1. (Added-AFMC) Baseline holdings:

A4.6.4.2. (Added-AFMC) Number of pages reviewed to date:

A4.6.4.3. (Added-AFMC) Number of pages reviewed to date:

A4.6.4.4. (Added-AFMC) Percent of baseline pages reviewed to date:

A4.6.4.5. (Added-AFMC) Number of pages declassified this period:

A4.6.4.6. (Added-AFMC) Number of pages declassified to date:

A4.6.4.7. (Added-AFMC) Number of pages downgraded this period:

A4.6.4.8. (Added-AFMC) Number of pages downgraded to date:

A4.6.4.9. (Added-AFMC) Number ofpages exempted this period:

A4.6.4.11. (Added-AFMC) Number of pages exempted to date:

A4.6.4.12. (Added-AFMC) -- 25X1 _____

A4.6.4.13. (Added-AFMC) -- 25X2 _____

A4.6.4.14. (Added-AFMC) -- 25X3 _____

A4.6.4.15. (Added-AFMC) -- 25X4 _____

A4.6.4.16. (Added-AFMC) -- 25X5 _____

A4.6.4.17. (Added-AFMC) -- 25X6 _____

A4.6.4.18. (Added-AFMC) -- 25X7 _____

A4.6.4.19. (Added-AFMC) -- 25X8 _____

A4.6.4.20. (Added-AFMC) -- 25X9 _____

A4.6.4.21. (Added-AFMC) TOTAL _____

A4.6.4.22. (Added-AFMC) - Number of referrals to date: _____

A4.6.4.23. (Added-AFMC) - Number of pages referred to date: _____

A4.6.4.24. (Added-AFMC) - Estimated cost for compliance to date: _____

Attachment 5

PHYSICAL SECURITY STANDARDS

A5.1. Intrusion Detection Systems (IDS) Standards. *[Reference DoD 5200.1-R, Appendix G, Paragraph B6]*

A5.1.1. Air Force IDS Standards. See AFI 31-101, Volume 1, **Air Force Physical Security Program**, Chapter 8, for Air Force policy on IDS.

A5.1.2. Trustworthiness Determinations. See AFI 31-501 for Air Force policy on trustworthiness determinations.

Attachment 6

TRANSMISSION TO FOREIGN GOVERNMENTS

A6.1. General. Air Force contracting officials ensure that US industrial activities have a government approved transportation plan or other transmission instructions.

Receipts. Air Force personnel: *[Reference DoD 5200.1-R, Appendix H, Paragraph a]*

A6.1.1. Use AF Form 349, **Receipt for Documents Released to Accredited Representatives of Foreign Nations** (available on the AFEPL);

A6.1.2. Show the complete unclassified title, description of a classified letter, minutes of meeting, and so on and any numerical identification of documents released on the form; and,

A6.1.3. Use the United States Postal System registered mail or Express Mail to transfer Secret or Confidential material to an embassy, official agency, or designated representative of the recipient foreign government in the United States.

A6.2. Whenever possible, shippers should use military airlift for shipping classified to foreign recipients. ***NOTE:*** When Air Mobility Command airlift can't deliver, determine an alternate secure method of direct delivery to a designated representative on a case-by-case basis. *[Reference DoD 5200.1-R, Appendix H, Paragraph c]*

A6.3. Depot and contract administration officials review lists of freight forwarders specified by the recipient foreign government to confirm that DoD 4000.25-8-M, *Military Assistance Program Address Directory System,* Jul 95**,** shows them as authorized to transport classified information.

A6.4. See AFPD 24-2 for instructions on "Report of Shipment."

A6.5. Overseas Shipments. See AFI 31-601 for Air Force policy on overseas shipments. *[Reference DoD 5200.1-R, Appendix H, Paragraph c(5)]*

A6.6. Foreign Military Sales (FMS). Air Force activities having primary management responsibility for processing foreign military sales cases ensure that personnel include transmission instructions. *[Reference DoD 5200.1-R, Appendix H, Paragraph e(1)(a)]*

Foreign military sales processors work with ISPMs and transportation officials on transportation plans submitted by foreign purchasers before giving final approval.

Attachment 7 (Added-AFMC)

AFMC ORIGINAL CLASSIFICATION AUTHORITIES

TOP SECRET AUTHORITIES	SECRET AUTHORITIES
HQ AFMC/CC	HQ AFMC/IN
AEDC/CC	AFFTC/CC
AAC/CC	HSC/XR
ASC/CC	DET 1, AFRL/WS
ESC/CC	WR-ALC/LF
OC-ALC/CC	WR-ALC/LK
OO-ALC/CC	WR-ALC/LN
AFRL/CC	WR-ALC/LU
AFRL/DE	WR-ALC/LY
SA-ALC/CC	AAC/WM
WR-ALC/CC	AFRL/MN
SM-ALC/CC	
SMC/CC	
AFRL/IF	
AFRL/ML	
AFRL/SN	
AFRL/VS	

Attachment 8 (Added-AFMC)

SECURITY CLASSIFICATION GUIDANCE

A8.1. (Added-AFMC) Program managers having primary management responsibility for a classified weapon system, plan, project, program (including a special access program), operation, equipment, or item (herein referred to as a system) must publish a formal SCG for each system they manage, if not peculiar to and previously published in another SCG. When changes are issued for an SCG, the guide must have a complete review. Identify the next biennial review date as 2 years from the date of the change. Submit DD Form 2024, **DOD Security Classification Guide Data Elements**, RCS: DD-C3I(AR)1418, IAW DoD 5200.1-R, Chapter 2, Section 5, paragraph 2-502; and AFI 31-401, paragraph 2.4.

A8.2. (Added-AFMC) Servicing ISPMs at each installation monitor the biennial review of SCGs issued by activities they service. They send a suspense notice to the 90 days before the review date. The OPR then issues changes as necessary. When major revisions to guides occur, the OPR must review for any change of performance and cost involved for the contractor in relationship to the current DD Form 254, **Contract Security Classification Specification.** Issue a revised DD Form 254, if these changes affect cost and performance. When changes to the basic SCG occur, the country-unique document OPR must evaluate them in order to update the existing document.

A8.3. (Added-AFMC) For SCGs sent to organizations or activities of other Air Force commands, provide a copy to the MAJCOM/SFA office and to HQ AFMC/SFXP.

A8.4. (Added-AFMC) Country-unique security classification documents (guides) developed in support of foreign governments or foreign contractor work performance and approved for release under National Disclosure Policy must contain a statement prohibiting release or disclosure of contents to third countries and their nationals.

A8.5. (Added-AFMC) SCGs are not releasable to foreign nationals or governments except as stated in A2.4 above. Use a DD Form 254 to convey contractual security classification guidance to foreign contractors. For procurement actions with complex security classification considerations, attach only those extracted portions of an approved SCG applicable to the foreign contractual performance to the DD Form 254, provided they are releasable to the foreign government under National Disclosure Policy.

A8.6. (Added-AFMC) Contractor participation in preparation of SCGs is encouraged. However, if more than one contractor is involved in performance of a contract, ensure all have the opportunity to comment and make recommendations for SCG changes.

A8.7. (Added-AFMC) Coordinate all security classification guides, changes, or revisions with the servicing ISPM before publication, except for guides containing sensitive compartmented information (SCI). Also, as appropriate, coordinate guides with the senior intelligence officer (SIO), Public Affairs, Foreign Disclosure, OPSEC and COMSEC officers.

A8.8. (Added-AFMC) Use one classification designation, e.g., U, C, S, or TS, under the classification column. Do not use U-TS, C-S etc. This forces the reader to make an original classification decision. Explain any differences in classification in the remarks column. The remarks column clarifies classification guidance when required.

A8.9. (Added-AFMC) The servicing ISPM classification management specialist keeps on file:

- A current DoD 5200.1-R and DOD 5200-1H.
- One copy of classification guides (and changes/revisions) issued by activities they service
- Related DD Forms 2024.
- Other SCGs necessary to support activities serviced.

A8.10. (Added-AFMC) See basic regulation, paragraphs 2-400, 5-206c and 5-302, for further guidance on applying the compilation rule and proper marking of documents.

A8.11. (Added-AFMC) The reason for assignment of distribution statements on the cover page for SCGs may be either Critical Technology or Specific Authority. Add distribution (AFI 61-204, *Disseminating Scientific and Technical Information*), reproduction limitation and destruction statements, as applicable, to guides. Deny FOIA requests for guides or unclassified extracts of classified guides according to 5 USC 552 (B)(2).

A8.12. (Added-AFMC) OCA signature is required on the "Foreword" page of the SCG. Record copy reflects OPR/program manager and servicing ISPM coordination.

A8.13. (Added-AFMC) Review distribution list upon revisions to SCGs to ensure only activities requiring SCGs are identified.

A8.14. (Added-AFMC) Revised SCGs and changes must contain a summary of changes, to include the topic or item changed. An OCA must approve and sign changes to guides involving classification decisions.

Attachment 9 (Added-AFMC)

SAMPLE TRAINING PLAN (ACTIVITY)

A9.1. (Added-AFMC) References:

a. DoDD 5000.1, *Defense Acquisition, para D.1.e*

b. DOD 52OO.l-R, *Information Security Program Regulation*

c. DOD 5200-1-PH, *A Guide To Marking Classified Documents*

d. DoD 5200.1M, *Acquisition Systems Protection Program/AFI 31-701*

e. DoDD 5230.11, *Disclosure of Classified Military Information to Foreign Governments and International Organizations*

f. AFI 10-1101, *Operations Security (OPSEC) Instructions*

g. AFI 31-209, *The Air Force Resource Protection Program*

h. AFI 31-210, *The Air Force Antiterrorism (AT) Program*

i. AFI 31-402, *Applying North Atlantic Treaty Organization (NATO) Protection Standards (pending)*

j. AFI 31-403, *Security Education Training and Awareness (pending)*

k. AFI 31-404, *USAF Security Classification Guide Database (pending)*

l. AFH 31-405, *USAF Information Security Program (pending)*

m. AFI 31-501, *Personnel Security Program Management*

n. AFI 31-601, *Industrial Security Program Management*

o. AFI 61-204, *Disseminating Scientific and Technical Information*

p. AFI 61-205, *Sponsoring or Co-Sponsoring, Conducting, and Presenting DOD-Related Scientific Papers at Unclassified and Classified Conferences, Symposia, and Other Similar Meetings*

q. AFI 71-101V1 and V2, *Criminal Investigations, Counterintelligence, and Protective Service Matters*

r. Executive Order 12958, *Classified National Security Information*

s. AFKAG 1, *COMSEC Responsibilities*

A9.2. (Added-AFMC) General. Commanders, staff agency chiefs and supervisors must ensure personnel understand the compelling need to protect classified and sensitive information, material and systems. To accomplish this, they ensure their personnel receive training as follows. All training areas may be expanded as determined locally: Initial Security Training is provided within 10 work days of a person physically assuming a position. This training will, as a minimum, cover subjects listed in DoD 5200.1-R, paragraph 9-200 and related subparagraphs. Special Requirements Training, as prescribed in DoD 5200.1-R, Chapter 9, Section 3, is presented within 30 days of an individual assuming a qualifying position. Security managers may present this training Thereafter, security managers provide Recurring and Refresher training. As a minimum, this training must be presented on a semi-annual basis, but quarterly sessions are recommended. Training via automated systems is the desired approach.

A9.3. (Added-AFMC) Schedule (Quarterly Recurring/Refresher Training)

a. **First session.**

(1) Security Program Roles and responsibilities

(2) Elements of classifying and declassifying information

(3) Elements of safeguarding

(4) Original classifiers' responsibilities and Classification Principles

(5) Declassification Standards and Methods

b. **Second session.**

(1) Original and derivative classification processes

(2) Classification markings

(3) Authorities, methods and processes for downgrading and declassifying information

(4) Methods for proper use, storage, reproduction, transmission, dissemination anddestruction of classified information

(5) Responsibilities of personnel serving as couriers of classified information.

c. **Third session.**

(1) Requirements for creating and updating classification/declassification guides

(2) Requirements for controlling access to classified information

(3) Procedures for investigating and reporting instances of security violations

(4) Sanctions for violating security directives/laws

(5) Protecting classified information stored in automated information systems

(6) Philosophies, requirements, and techniques embodied in the Industrial Security Program.

d. **Fourth session.**

(1) Requirements for creating, maintaining, and terminating special access programs

(2) Mechanisms for monitoring special access programs

(3) Practices applicable to U.S. officials traveling overseas

(4) Requirements for oversight of the security classification program, including self inspections

(5) The threat and techniques employed by foreign intelligence activities attempting to obtain classified information.

APPROVED

_____ _____

Commander/Staff Agency Chief Signature Date